Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 3 (березень)

Київ – 2018

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В. І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л.Литвинова. Дизайн обкладинки С.Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

ЗМІСТ

«Украинский хактивист, известный как Dmitry Orlov, обнаружил в открытом доступе чертежи и документы, используемые украинским заводом «Маяк» для производства оружия…

ПАО «Завод «Маяк» входит в государственный концерн «Укрборонпром». Согласно официальному сайту завода, основными направлениями его деятельности являются разработка и производство стрелкового оружия (снайперских винтовок, пехотных и танковых пулемётов), артиллерийского оружия, модернизация и ремонт колесной бронетехники, экспорт и импорт продукции военного и специального назначения.

…в общем доступе различные чертежи оказались благодаря открытому для всех желающих сетевому диску с данными.

В ПАО «Завод «Маяк»… сообщили, что обнародованные хактивистами данные не являются секретными:

– Это обычная рабочая информация, никаких секретных данных там нет, – отметили в ПАО «Завод «Маяк».

В то же время ответить на вопрос, закрыта ли уязвимость на данный момент и обнаружен ли вообще источник утечки нашему журналисту не смогли, попросив предоставить письменный запрос…» ***(Владимир Кондрашов. Документы украинского производителя оружия обнаружены в открытом доступе // Internetua (http://internetua.com/dokument-ukrainskogo-proizvoditelya-orujiya-obnarujen-v-otkrtom-dostupe). 26.02.2018).***

***

«Американська транснаціональна корпорація Cisco спільно з ГО «Вікімедіа Україна» оголошує конкурс «Пишемо про інформаційну безпеку»…

Згідно документу, мета проекту — наповнити Вікіпедію актуальними статтями про технології інформаційної безпеки українською мовою. Конкурс триватиме з 1 по 30 квітня 2018 року. У цей період усі охочі зможуть долучитися до написання, перекладу чи доповнення статей із запропонованого організаторами списку, а також до створення оригінальних матеріалів…

Участь у конкурсі може взяти будь-який зареєстрований користувач Вікіпедії. Для цього потрібно створити або доповнити статтю на сторінці конкурсу…

Журі, яке складається з ентузіастів української Вікіпедії, перевірятиме конкурсні статті у травні, після чого будуть оголошені переможці…» ***(Cisco і українська Вікіпедія оголосили конкурс матеріалів про інформаційну безпеку // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/270318-cisco-i-ukrayinska-vikipediya-ogolosyly-konkurs-materialiv-pro-informaciynu-bezpeku). 27.03.2018).***

***

«Україна завершує створення центрів реагування на кіберзагрози в державній інформаційній інфраструктурі…

Про це заявила віце-прем'єр-міністр з питань європейської та євроатлантичної інтеграції України Іванна Климпуш-Цинцадзе в ході зустрічі з заступником Генерального секретаря НАТО з нових викликів безпеці Антоніо Міссіролі в Брюсселі…

«МЗС України перебуває на передовій кібератак. Сподіваюся, найближчим часом буде представлено спільний підхід до вирішення проблематики цієї сфери…», – стверджує Климпуш-Цинцадзе.

У свою чергу заступник Генерального секретаря НАТО з нових викликів безпеці Антоніо Міссіролі зазначив, що альянс добре розуміє ті виклики, які стоять перед Україною, і усвідомлює необхідність якісної міжурядової кооперації та комунікацій…» ***(Україна завершує створення центрів реагування на кіберзагрози // kherson-news.info (http://kherson-news.info/politics/ykrayina-zavershyye-stvorennia-centriv-reagyvannia-na-kiberzagrozi/). 10.03.2018).***

***

«В Минэнергоугля заявили об угрозах кибербезопасности объектов инфраструктуры. Украина может присоединиться к центру энергетической безопасности НАТО в 2018 году.

Об этом на инновационном форуме по информационно-коммуникационным технологиям сообщила замглавы Министерства энергетики и угольной промышленности по вопросам европейской интеграции Наталья Бойко…

Она также назвала приоритетом обеспечение кибербезопасности объектов инфраструктуры.

…В то же время посол Литвы в Украине Мариус Януконис отметил, что странам следует использовать все возможности, которые предоставляют ЕС и НАТО в сфере кибербезопасности» ***(Украина рассчитывает на присоединение к центру энергетической безопасности НАТО в 2018 // Citynews.Net.UA (http://www.citynews.net.ua/ukrainenews/70907-ukraina-rasschityvaet-na-prisoedinenie-k-centru-energeticheskoy-bezopasnosti-nato-v-2018.html). 07.03.2018).***

***

«…Кількість вірусних заражень і хакерських атак в Україні за останній рік зросла з 10 мільйонів до 100 млн.

Про це сказав експерт в галузі інформаційної безпеки Володимир Ілібман під час презентації звіту Cisco з кібербезпеки…

«Із року в рік кількість атак та вірусів зростає… Але є добра новина — ми, компанія Cisco, скорочуємо час реагування на них. Якщо у 2015 році від початку нової атаки до реагування йшло 37 годин, то у 2017 році — 4 години», — сказав Ілібман.

За його словами, нині спостерігається безпрецедентний рівень технічної складності і руйнівного впливу хакерських атак…

«…Хакери застосовують мережні віруси-здирники, використовують шифрування та використовують усе те, що ІТ-компанії використовують для захисту, але з іншою метою», — сказав експерт.

На думку Ілібмана, фахівці з ІТ-безпеки мають більше інвестувати у захист своїх організацій» ***(В Україні здійснили 100 мільйонів хакерських атак // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/v-ukrayini-zdiysnili-100-milyoniv-hakerskih-atak.html). 14.03.2018).***

***

«…в одиннадцати из 24 украинских облэнерго значительной долей владеет российский националист Александр Бабаков. Он находится под санкциями за роль в российской оккупации и аннексии Крыма…», - заявил аналитик Atlantic Council Андерс Аслунд…

Аналитик советует Украине заморозить активы российского националиста учитывая вопросы национальной безопасности.

«Мы заботимся из-за российских кибератак на украинские энергосети. Это в то время, как значительной ее частью владеет, контролирует и управляет враг», - говорит он.

Кроме Бабакова, еще одним владельцем является Константин Григоришин. Ранее был российским гражданином. Сейчас получил украинское гражданство» ***(Эксперт предупредил об угрозе национальной безопасности в энергоснабжении // Gazeta.ua (https://gazeta.ua/ru/articles/economics/_ekspert-predupredil-ob-ugroze-nacionalnoj-bezopasnosti-v-energosnabzhenii/829124). 30.03.2018).***

***

Правове забезпечення кібербезпеки в Україні

«Национальная комиссия, осуществляющая госрегулирование в сфере связи и информатизации, на заседании сегодня, 6 марта, высказалась за целесообразность принятия проекта Закона Украины «О внесении изменений в Закон Украины «О санкциях».

Законопроект № 8042 (от 15.02.2018), внесенный в раду Кабмином, вводит запрет или ограничение использования на объектах критической инфраструктуры программного обеспечения и технических средств из страны, которая находится под санкциями…

Под запрет попадут ПО и технические средства из иностранного государства, к которому применены санкции, либо разработанные/изготовленные юридическим лицом-резидентом иностранного государства, или юридическим лицом, доля уставного капитала которого находится в собственности иностранного государства, или юридическим лицом, находящимся под контролем юридического лица иностранного государства.

…Во время общественного обсуждения законопроекта были получены позиции по документу от Телекоммуникационной палаты Украины и Украинского союза промышленников и предпринимателей, суть которых сводится к

нецелесообразности принятия законопроекта» ***(Владимир Кондрашов. Власти хотят отказаться от российского ПО на объектах критической инфраструктуры // Internetua (http://internetua.com/vlasti-hotyat-otkazatsya-ot-rossiiskogo-po-na-ob-ektah-kriticseskoi-infrastruktur). 06.03.2018).***

***

«Президент України вніс на розгляд Верховної Ради законопроект про національну безпеку.

Проект закону містить п’ять розділів…

Розділ V регулює планування у сфері національної безпеки і оборони, визначає основні документи довгострокового планування, зокрема Стратегію національної безпеки України, Стратегію воєнної безпеки України, Стратегію громадської безпеки та цивільного захисту України, Стратегію розвитку оборонно-промислового комплексу України, Стратегію кібербезпеки України, Національну розвідувальну програму, також порядок їх формування та реалізації у документах середньострокового та короткострокового планування» ***(Президент вніс у Раду законопроект про нацбезпеку // Інформаційно-правовий портал «Українське право» (http://ukrainepravo.com/news/ukraine/prezydent-vnis-u-radu-zakonoproekt-pro-natsbezpeku/). 05.03.2018).***

***

«…Профильный комитет по вопросам информатизации и связи не поддержал и отправил на доработку ЗП "О санкциях" реестр. № 8042 от 15.02.2018. Хотя профильный комитет не основной, но будем от общественности поддерживать позицию комитета», – написал на своей странице в Facebook сообщил Глава Правления Интернет Ассоциации Украины Александр Федиенко

…представители отрасли также обратили внимание на то, что фактически документ, который был разработан в ДСТЗИ, и тот, который пошел в комитеты на согласование, имеют различные формы построения…» ***(Владимир Кондрашов. Профильный комитет Рады не поддержал запрет российского ПО // InternetUA (http://internetua.com/profilni-komitet-rad-ne-podderjal-zapret-rossiiskogo-po). 16.03.2018).***

***

«Законом України «Про основні засади забезпечення кібербезпеки України» телекомунікаційні мережі та системи всіх форм власності, в яких обробляють національні інформаційні ресурси та/або які використовують в інтересах органів державної влади, місцевого самоврядування, правоохоронних органів та військових формувань, а також комунікаційні системи, які використовують для технологічних потреб енергетики, транспорту, промисловості, задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу, визначені об’єктами критичної інфраструктури держави…

Для забезпечення сталого функціонування телекомунікаційних мереж та їх захисту від кіберзагроз (як у звичайних умовах мирного часу, так і в умовах надзвичайних ситуацій, надзвичайного та воєнного стану) створюється Система оперативнотехнічного управління телекомунікаційними мережами (СОТУ).

…Основні критерії для визначення телекомунікаційних мереж об'єктами управління СОТУ такі:

• розгалуженість цих мереж та покриття всієї території України або значної її частини, велика потужність та достатні надійність і живучість;

• сучасний технологічний рівень і постійний розвиток;

• висока якість телекомунікаційних послуг та велика абонентська база;

• наявність достатнього мережевого ресурсу, зокрема незадіяного (волокон, каналів, трактів), який можна використати в умовах надзвичайних ситуацій і який забезпечить мобілізаційну готовність в особливий період;

• наявність власних центрів управління мережами, високий рівень технічної експлуатації.

Головне місце в загальній структурі об'єктів управління СОТУ займає Національна телекомунікаційна мережа (НТМ)…

Центральний суб'єкт у СОТУ — НЦУ…

Важлива умова створення і забезпечення функціонування СОТУ та НЦУ — наявність ефективної нормативно-правової та нормативно-технічної бази. На основі проведених досліджень Держспецзв'язку підготовлено проекти нормативно-правових актів і нормативних документів. Один з найважливіших проектів — Загальні технічні вимоги до складових системи оперативно-технічного управління телекомунікаційними мережами…

У Держспецзв'язку відповідно до планів роботи та передбачених коштів уже розпочато проведення циклу науково-дослідних, дослідно-конструкторських, проектних та будівельних робіт, у результаті яких буде створено першу чергу апаратно-програмного комплексу інформаційно-аналітичної системи (ІАС) НЦУ, побудовано та введено в дослідну експлуатацію пусковий комплекс (першу чергу) СОТУ та НЦУ. Дослідний зразок ІАС першої черги НЦУ розташують у спеціально обладнаному приміщенні із забезпеченням умов, які буде визначено для пускового комплексу (першої черги) об'єкта «Будівництво основного НЦУ»…

Введення пускового комплексу НЦУ у дослідну експлуатацію заплановано на листопад цього року…» ***(Леонід ЄВДОЧЕНКО, Олександр ДАНЧЕНКО, Олександр ЖИВОТОВСЬКИЙ, Олександр ЧАУЗОВ, Петро КОВАЛЬОВ. Про об'єкти критичної інфраструктури та управління телекомунікаціями // «Урядовий кур'єр» (http://ukurier.gov.ua/uk/articles/pro-obyekti-kritichnoyi-infrastrukturi-ta-upravlin/). 15.03.2018).***

***

«…Нещодавно Нацкомісія з регулювання зв'язку та інформатизації схвалила законопроект… «Про внесення змін до деяких законодавчих актів України щодо імплементації положень Конвенції про кіберзлочинність». …Громадські організації, експерти,оператори зв'язку та деякі чиновники вже б'ють

на сполох. Документ порушує чималу кількість міжнародних стандартів щодо забезпечення права особи на приватність.

..згідно з законопроектом правоохоронні органи зможуть через інтернет-провайдерів та операторів мобільного зв'язку збирати інформацію щодо громадян та зберігати її. Крім того документ значно спрощує процедуру блокування будь-якого веб-сайту та інтернет-ресурсу на невизначений термін.

Скандальну ініціативу розробили у кіберполіції… За інформацією джерел «Главкома», на такому варіанті наполягли у МВС…

Мета законопроекту – встановити правила гри та базові норми, які характерні для європейських країн. Глава кіберполіції Сергій Демедюк зазначає, що Нацполіція має намір допрацьовувати проект, враховуючи зауваження учасників ринку. Демедюк переконує, норми законопроекту, зокрема щодо блокування сайтів, вже працюють в європейських країнах і незабаром будуть внесені до Конвенції…

Варто сказати, що законопроект складається з декількох частин, які частково суперечать одна одній. Перша частина передбачає зміни до деяких законів, друга – до Кримінального кодексу України, третя – до закону «Про телекомунікації».

Найсуперечливіша норма законопроекту – можливість блокування веб-сайтів слідчим суддею …без участі у засіданні власника… на строк до 90 днів з можливістю подовжити його до трьох років…

За словами експерта Лабораторії цифрової безпеки Вадима Гудими, така норма законопроекту створює широке поле для зловживання владою та введення жорсткої цензури під егідою поліції…

У третій частині документу знову йде мова про блокування, але вже не на підставі рішення слідчого судді, а лише за приписом «суб'єктів національної системи кібербезпеки», а до цього переліку входять Національна поліція, СБУ, Міноборони, Держспецзв'язку, Служба зовнішньої розвідки України та навіть Нацбанк. І вже у цій частині закону будь-які згадки про строки блокування сайтів відсутні, а значить їх зможуть заблокувати безстроково…

Варто сказати, у Нацкомісії, що здійснює державне регулювання у сфері зв'язку та інформатизації хоч підтвердили законопроект, але вважають, що блокувати потрібно тільки заборонену інформацію, а не весь ресурс, на якому цю інформацію розміщено, як передбачається в законопроекті. Адже так може бути заблокована законна інформація або інший ресурс, який використовує один домен спільно з правопорушником, нарікає регулятор.

За законопроектом, оператори зв'язку будуть зобов'язані формувати «кінцевий список користувачів» (такого терміну в українському законодавстві не існує, це, за словами експертів, ще одна колізія) зберігати його та надавати правоохоронцям, якщо вони того вимагатимуть…

За словами експертів, під поняттям «кінцевий список користувачів» можуть розумітися не лише персональні дані користувачів (які, до речі, мають бути захищені публічною офертою, яку укладають користувач і провайдер), а й весь інтернет-трафік людини, тобто все, що вона шукала і робила у мережі. Ці дані оператор змушений буде зберігати від 90 днів з можливістю подовжити цей строк до трьох років. Чому саме такий термін, у законопроекті не пояснюється…

У Нацкомісії, що здійснює державне регулювання у сфері зв'язку та інформатизації стверджують , що норму, яка зобов'язує провайдерів формувати список кінцевих користувачів, потрібно переглянути…

Громадські організації говорять про те, що законопроект суперечить рекомендаціям Комітету міністрів Ради Європи щодо прав інтернет-користувачів, які базуються на Європейській конвенції про захист прав людини.

Встановлення засобів загального спостереження та/або перехоплення інформації в мережі інтернет прямо суперечить Рекомендаціям CM/Rec(2014)6 Комітету міністрів Ради Європи…

Йдеться про те, що держава не може встановлювати механізми та загальний контроль над громадянами, а на порушення у кіберпросторі має регувати точково – закривати лише певний сайт або слідкувати лише за певною людиною, яка підозрюється у вчиненні злочину…

Народний депутат та голова комітету з питань інформатизації та зв'язку Олександр Данченко, який нещодавно повернувся з кіберсаміту у Будапешті, переконаний, що …швидше за все, новий скандальний документ про кіберзлочинність врешті-решт можуть навіть не зареєструвати у Верховній Раді…» ***(Юлія Тунік. «Роскомнадзор» по-українськи. Як кіберполіція підставила уряд // Vse.Media (http://vse.media/roskomnadzor-po-ukrayinski-yak-kiberpolitsiya-pidstavila-uryad/). 22.03.2018).***

***

Кібервійна проти України

«Гібридний характер агресії Росії проти України підкреслюють кібератаки, здійснювані росіянами. Про це в телепрограмі Державного департаменту США Readout сказав заступник державного секретаря Джон Салліван… Процес реформування в Україні надзвичайно ускладнюється зовнішньою агресією та іншими загрозами, що виходять з РФ, зазначив заступник держсекретаря. "Це не тільки військова операція, а й кібероперації… Ми вважаємо, що росіяни використовують Україну як лабораторії для такого виду шкідливих дій", – підкреслив Салліван» ***(Кремль тестує на Україні кібероперації для всього світу // ТзОВ "Редакційні системи" (http://expres.ua/news/2018/03/08/286958-kreml-testuye-ukrayini-kiberoperaciyi-vsogo-svitu). 08.03.2018).***

***

«Неизвестные хакеры с помощью аккаунтов-клонов и фэйковых блогов пытаются дискредитировать деятельность Украинских кибервойск и их основателя Евгения Докукина.

Как сообщает спикер Украинского Киберальянса, известный под ником Sean Brian Townsend, неизвестные взламывают сайты в Беларуси от имени Украинских Кибервойск и Евгения Докукина и постят новости об этом в аккаунт-«клон» УКВ в Twitter.

Также украинские хактивисты обнаружили поддельный блог, копирующий блог Евгения Докукина…

Основатель Украинских кибревойск сообщил, что со вчерашнего дня пытается заблокировать «свои» фейковые аккаунты, но пока площадки не реагируют на его обращения…

Sean Brian Townsend указывает на активизацию сил страны-агрессора, направленных, в том числе, на дискредитацию украинского волонтерского киберсообщества. Ранее на почтовые адреса InformNapalma пришло подозрительное письмо с предложением продать массив информации, полученный в результате взлома офицеров МО РФ и спецслужб:

– Кому-то очень было нужно, чтобы эта информация попала в паблик… Как по мне, так это начало, какого-то активного мероприятия со стороны наших северных соседей, – считает Sean Brian Townsend…» ***(Владимир Кондрашов. Неизвестные взламывают сайты в Беларуси от имени Украинских кибервойск // InternetUA (http://internetua.com/neizvestne-vzlamvauat-sait-v-belarusi-ot-imeni-ukrainskih-kibervoisk). 15.03.2018).***

***

«В последние годы Украина стала полигоном для испытания кибероружия и новых форм кибератак, а точнее – даже полем кибербитвы. Так произошло потому, что мы это позволили. Наша киберзащита еще до войны была на объективно слабом уровне. И не только потому, что ей никто не занимался на государственном уровне, а потому что многие подобные процессы контролировались силами, которые были не заинтересованы в действенной системе национальной безопасности Украины, а скорее наоборот…

С каждой новой атакой к украинским компаниям и государству приходит осознание того, что кибербезопасность – важная составляющая нацбезопасности…

При этом просто захотеть и стать лидером в кибербезопасности на мировом уровне невозможно, особенно в стране с низким уровнем жизни и недостаточным финансированием данной сферы или конкретного проекта… Простым языком, это дорого и, кроме того, не совсем логично – своими силами создавать «мировой центр кибербезопасности». Другое дело – организовать такой институт в Украине при содействии мирового сообщества, что стало бы хорошим решением для нашей страны» ***(Владислав Андрианов. Украина как мировой центр кибербезопасности. Почему нет? // Дом инноваций (https://innovationhouse.org.ua/ru/columns/ukrayna-kak-myrovoj-tsentr-kyberbezopasnosty-pochemu-net/). 16.03.2018).***

***

«Співробітники Служби безпеки України спільно з Генпрокуратурою викрили у Києв і діяльність офісу прокремлівських хакерів.

Оперативники спецслужби встановили, що підконтрольне ФСБ хакерське угруповання організовувало кібератаки, зокрема на об’єкти критичної інфраструктури, державні та банківські установи. Для приховування ідентифікації атак зловмисники використовували сервіси анонімізації повідомлень.

Співробітники СБ України також задокументували, що зловмисники за вказівкою російських спецслужб задіювали так звані «бот-ферми» для проведення спеціальних інформаційних операцій проти нашої країни.

Під час обшуків в офісі та за місцями проживання фігурантів справи правоохоронці виявили програмно-апаратні комплекси, серверне обладнання, комп'ютерну техніку та понад п'ятдесят тисяч карток мобільних операторів різних країн, задіяних у хакерських атаках.

Триває досудове розслідування у рамках кримінального провадження, відкритого за ст. 361 Кримінального кодексу України» ***(СБУ блокувала у Києві діяльність офісу прокремлівських хакерів // Народна Рада (http://narodnarada.info/news/sbu-blokuvala-kievi-diyalnist-ofisu-news-94172.html). 23.03.2018).***

***

«**Північноатлантичний альянс може допомогти Україні у забезпеченні стійкості та захищеності електронної системи Центрвиборчкому від зовнішнього втручання під час проведення виборів у 2019 році.**

Про це заявила віце-прем'єр-міністр з питань європейської та євроатлантичної інтеграції України Іванна Климпуш-Цинцадзе за результатами засідання Комісії Україна-НАТО, що відбулося напередодні у Брюсселі…

Климпуш-Цинцадзе повідомила, що з відповідною пропозицією на засіданні КУН виступила Румунія, яка є головною нацією у трастовому фонді з допомоги НАТО у питанні кібербезпеки…

За словами урядовця, ЦВК може бути залученою до програм, які фінансує фонд.

Климпуш-Цинцадзе зазначила, що українська сторона зацікавлена, щоб ця кіберініціатива була реалізована до початку проведення виборів в Україні у 2019 році» ***(НАТО допоможе Україні захиститися від зовнішнього втручання у вибори-2019 // Західна інформаційна корпорація (https://zik.ua/news/2018/03/29/nato_dopomozhe_ukraini_zahystytysya_vid_zovnishnogo_vtruchannya_u_vybory2019_1295185). 29.03.2018).***

***

«Примерно месяц назад украинская киберкоманда CERT-UA опубликовала сообщение о массовой рассылке фишинговых писем, в которых содержались ссылки на загрузку вредоносных файлов. Детальный анализ кибератаки дал все основания полагать, что она была проведена по заказу спецслужб северного соседа, наиболее вероятно - хакерами из группы Fancy Bear, деятельность которой отвечает интересам российских властей.

И, как оказалось, это далеко не первая целевая кибератака со стороны РФ…

Подробная информация о целях, которые были атакованы хакерской группой Fancy Bear, поступила от компании Secureworks, дочернего предприятия Dell Technologies, специализирующееся на кибербезопасности. Всего с марта 2015 по май 2016 были атакованы 4705 электронных адресов. Хакеры присылали на

указанные электронные ящики фишинговые письма или письма, содержащие зараженные файлы.

Далее все данные о таких кибератаках Secureworks передал международному информационному агентству Associated Press, где их анализом занялся журналист Рафаэль Саттер (Raphael Satter). Он проанализировал весь перечень и обнаружил среди них по меньшей мере 554 украинских адресатов.

В рамках этой группы были 213 целей - журналисты, активисты и другие деятели гражданского общества, 159 - государственные деятели (государственные служащие, дипломаты и депутаты), еще 75 - военнослужащие (военные атташе, старшие офицеры или добровольцы). Остальные - работают в частных бизнес-структурах, или же их нельзя классифицировать однозначно…

Анализ выбранных целей говорит о том, что хакеры атаковали вовсе не случайных людей. Почти все они занимались определенной политической или общественной деятельностью…

Предыдущие отчеты Associated Press показали, что Fancy Bear использовал фишинговые электронные письма, чтобы скомпрометировать лидеров российской оппозиции, украинских политиков и американских разведчиков, а также руководителя избирательной кампании Хиллари Клинтон Джона Подеста и более 130 других членов демократической партии…» ***(Олег Релипенко. Российские кибератаки на украинских волонтеров // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/228713-rossijskie_kiberataki_na_ukrainskih_volonterov). 27.03.2018).***

***

Боротьба з кіберзлочинністю в Україні

«В конце сентября прошлого года Нацполиция отчиталась о задержании 40-летнего жителя Киевской области, который за деньги сбывал в сети Интернет персональные данные украинцев. На днях Бориспольский горрайонный суд Киевской области поставил точку в этом резонансном деле.

Решение суда и заявления Нацполиции очень сильно расходятся в фактах и масштабах происшедшего…

27 сентября Департамент киберполиции НПУ отчитался о задержании экс-сотрудника ГУ Пенсионного фонда в Киевской области…

По данным полиции, на компьютере злоумышленника было обнаружено 250 баз данных, запрещенных в свободном доступе и охраняемых законом. Тогда начальник Киевского управления киберполиции Сергей Кропива рассказывал о том, что его подопечные выявили пользователя, рекламирующего в сети услуги по распространению и продаже различных баз данных, в которых хранилась персональная информация украинцев…

По данному факту Следственным управлением полиции Киевской области было открыто уголовное производство по признакам состава преступлений, предусмотренных статьей 362 ККУ (несанкционированные действия с информацией) и проводилось досудебное расследование...

В решении суда никоим образом не упоминаются 250 баз данных, якобы обнаруженных у подозреваемого, и нет ни слова об их продаже или сбыте, а «обнаруженная вся сетевая и компьютерная техника, с помощью которой осуществлялось распространение баз данных» превратилась в одно вещественное доказательство – моноблок «Lenovo».

«Громкое дело» о владельце 2,5 сотен баз персональных данных, якобы продающем их даже стране-агрессору, превратилось в «обычное» преступление среднего пошиба: сотрудник Пенсионного фонда в Киевской области 25 января 2016 года скопировал с Автоматизированной системы обработки пенсионной документации на базе компьютерных технологий информацию о выданных пенсионных удостоверениях ГУ ПФУ в Киевской области. Позже на ресурс, «специализирующийся» на продаже и обмене незаконных баз данных, злоумышленник с ником «hatmaster» загрузил информацию под названием «Киевская обл. пенсионные удостоверения-2008-2014» для публичного доступа и осмотра.

Ресурс, между прочим, работает до сих пор. О судьбе других баз данных в решении суда не упоминается.

Отметим, что все данные, на которые опирался суд, были получены благодаря тому, что житель Киевской области пошел на сделку со следствием…

Суд, принимая во внимание соглашение о признании вины, назначил обвиняемому наказание в виде 2 лет лишения свободы с лишением права занимать определенные должности или заниматься определенной деятельностью в органах Государственной власти Украины и местного самоуправления Украины сроком на 2 года. В зале суда обвиняемый был освобожден от наказания с испытательным сроком на год. На основании Закона Украины «Об амнистии в 2016 году» мужчина был освобожден от отбывания назначенного основного и дополнительного наказания…» ***(Владимир Кондрашов. Как «торговец персональными данными» оказался в суде ни в чем не виноват // Internetua (http://internetua.com/kak-torgovec-personalnmi-dannmi-okazalsya-v-sude-ni-v-csem-ne-vinovat). 06.03.2018).***

***

«…Уроженец Котовска Одесской области после увольнения с должности инженера по защите информации службы безопасности ООО «Померанч», несмотря на соглашение о соблюдении коммерческой тайны с работодателем, начиная с мая прошлого года, незаконно получал доступ к административной панели видеорегистраторов, … являющихся собственностью ООО «Померанч», в Одессе, Киеве, Днепре, Харькове и Запорожье…

Часть записей с камер видеонаблюдения в Одессе и Киеве злоумышленник просто скопировал себе, а из части записей смонтировал более десятка видеороликов (записей с Киева – Крещатик, 50 и ТЦ «Глобус», Днепра – ТЦ «Караван» и Запорожья – ТЦ «СитиМол»), которые загрузил в сеть. Куда именно загружались видео, не сообщается, как и, собственно, мотивация их создателя.

Суд посчитал, что своими умышленными действиями экс-сотрудник «Померанча» совершил уголовные преступления, предусмотренные ч.1 и ч.2 ст.361 УК Украины, ч.2 и ч.3. ст.362 УК Украины, ч.1 и ч.2 ст.361-2 УК Украины.

Учитывая смягчающие обстоятельства (искреннее раскаяние, активное способствование раскрытию преступлений, положительная характеристика, отсутствие вреда), суд признал уроженца Котовска виновным и присудил три года лишения свободы с испытательным сроком на год и конфискацией техсредств…» ***(Владимир Кондрашов. Экс-сотрудник «Цитруса» получил три года за видеоролики с камер наблюдения // Internetua (http://internetua.com/eks-sotrudnik-citrusa-polucsil-tri-goda-za-videoroliki-s-kamer-nabluadeniya). 02.03.2018).***

***

«…хакер (в сети называл себя «AntonShesar» и «Catona») занимался созданием и сбытом вредоносного программного обеспечения, предназначенного для вмешательства в работу серверного оборудования, и получения доступа к базам данных, которые на нем находятся, сообщили в Департаменте киберполиции Национальной полиции.

В целях конспирации хакер размещал ссылки на загрузку разработанного им вируса на веб-ресурсе, который находился на территории Российской Федерации. Управление вирусом осуществлялось с использованием удаленного RDP протокола.

Сообщается, что злоумышленнику 22 года, и он житель Черкасской области.

Также полицейскими установлено, что мошенник на различных хакерских форумах предлагал свои услуги по предоставлению в аренду вредоносных программ. При этом его покупателями могли быть как отечественные, так и иностранные мошенники…

Полицейскими проведено одновременно три обыска на территории Черкасской и Киевской областей…

Следователи обнаружили файлы, подтверждающие, что мошенником было скомпрометировано более 5 тыс. учетных записей. Кроме того, на дополнительных носителях информации выявлено информацию о 10 тыс. учетных записях электронных ящиков, доступ к которым был получен незаконно…

Продолжается досудебное расследование в рамках начатого уголовного производства по ст. 361 УК Украины (несанкционированное вмешательство в работу компьютерных сетей)» ***(Сергей Савенко. Киберполиция разоблачила хакера, который создавал для продажи компьютерные вирусы // Internetua (http://internetua.com/kiberpoliciya-razoblacsila-hakera-kotori-sozdaval-dlya-prodaji-kompuaterne-virus). 30.03.2018).***

***

«…Приватбанк у 2017 році виплатив 512 тис. гривень винагороди "білим хакерам", які допомогли йому виявити вразливості в кібербезпеці…

Минулого року грошову премію від Приватбанку заслужили 127 комп’ютерних фахівців, які посприяли усуненню потенційних "дірок" в електронних системах компанії. Щоби полегшити взаємодію з "білими хакерами", банк у березні 2018 року відкрив спеціальний сайт…

Згідно з повідомленням прес-служби, Приватбанк у 2012 році став першою у світі банківською установою, яка почала виплачувати винагороду (до $1 тис.) за

пошук вразливостей у своїх інтернет-системах» ***(Білі хакери отримали від Приватбанку понад 0,5 млн гривень // Молодий буковинець (https://molbuk.ua/ukraine/146296-bili-khakery-otrymaly-vid-pryvatbanku-ponad-05-mln-gryven.html). 17.03.2018).***

***

«…Не чистые на руку хакеры, вместо того чтобы использовать мощности только собственного компьютера, начинают тайно подключаться к чужим ПК и зарабатывать на них деньги.

Сайт госгидромецентра – это первоисточник информации о погоде, поэтому посещает его многие. …на прошлой неделе …кто-то установил на сайт вирус, который использовал мощности пользователей, чтобы майнить криптоваплюту.

Из-за скрытого майнинга процессор посетителей работал почти на 100 процентов, а следовательно электроэнергии тратил больше. К тому же компьютер начинал зависать. Злоумышленники, которые устанавливали вирус, даже не пытались его скрыть. Поэтому обнаружили проблему быстро.

…Специалист по кибербезопасности Егор Папишев за несколько минут находит еще целый ряд сайтов, на украинских доменах, которые успешно майнят имущество на своих посетителях…» ***(Скрытый майнинг в Украине: как массово воруют криптовалюту // АНТИКОР — национальный антикоррупционный портал(https://antikor.com.ua/articles/226942-skrytyj_majning_v_ukraine_kak_massovo_vorujut_kriptovaljutu). 17.03.2018).***

***

«… хакерская группа LisardSquad рассылает письма, в которых "уведомляет" компании о предстоящих кибератаках.

Об этом сообщает пресс-служба Департамента киберполиции.

Для предотвращения "запланированной" кибератаки, злоумышленники требуют заплатить им 3 BTC (биткойна). В случае неуплаты, комиссия увеличивают на 5 BTC за каждый день "просрочки".

Специалисты Департамента проводят необходимые розыскные мероприятия и подчеркивают, что перечисление средств не гарантирует полноценную защиту от атак. Эффект данных писем усиливается еще и тем, что в последнее время наблюдается все больше случаев использования нового вектора DDoS-атак - через протокол Memcached.

Эксперты советуют администраторам серверов с указанным протоколом следующее:

проверить факт наличия уязвимости в конфигурациях сервиса;

убедиться, что протокол Memcached прослушивает исключительно локальный интерфейс или только те интерфейсы, которые не имеют прямого доступа к Интернету, а также защищены соответствующими настройками фаервола;

включить систему логирования, чтобы фиксировать все факты вмешательства в работу серверов Memcached посторонних лиц…» ***(Хакеры начали шантажировать украинские компании кибератаками, требуя биткоины за***

защиту // "INSIDER LIFE NEWS" (http://ilife-news.com/57835-hakery-nachali-shantazhirovat-ukrainskie-kompanii-kiberatakami-trebuya-bitkoiny-za-zaschitu.html). 17.03.2018).

***

«Интернет-холдингу Dating.com Group совместно с Group-IB и Qrator Labs удалось вычислить и привлечь к судебной ответственности украинскую хакерскую группу, занимавшуюся вымогательством и проведением DDoS-атак на международные интернет-компании в течение двух лет.

В результате совместной работы по предотвращению атаки, установлению личностей участников хакерской группы и сбору доказательств для судебного преследования на Украине создан первый в истории прецедент по установлению полной меры уголовного наказания за киберпреступление.

В 2015 и 2016 гг. один из проектов холдинга Dating.com Group – международный сервис онлайн-знакомств AnastasiaDate – столкнулся с мощными повторяющимися DDoS-атаками. Они вызвали многочасовые перебои в работе и отказ в обслуживании сайта компании. Каждый раз с представителями компании связывались организаторы атак и требовали вознаграждение за прекращение нападений на ресурс: с каждой атакой сумма увеличивалась в несколько раз.

Служба безопасности интернет-холдинга Dating.com Group обратилась к специалистам Group-IB за помощью в установлении личностей участников хакерской группы причастных к организации DDoS. Эксперты отдела расследований Group-IB проанализировали цифровые следы атаки и установили не только личности злоумышленников, но и цепочку других инцидентов, следы которых вели к тем же вымогателям…» ***Украинские организаторы DDoS-атак получили срок // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5480321-Kiberprestupniki-organizovavshie.html#ixzz5AC1shK3P). 14.03.2018).***

***

«Только за прошлый год мировая экономика потеряла из-за киберперступников около $600 млрд, а еще несколько лет назад эта цифра была на уровне $445 млрд.

…несколько простых рекомендаций позволят минимизировать риски. Самое простое решение - завести отдельную карту для интернет-платежей (например, виртуальную)…

Чаще всего "утечка" информации происходит с скомпрометированного или поддельного сайта, на котором произвели платеж, либо с самого компьютера с помощью вредоносной программы. Главный совет –пользоваться известными и надежными онлайн-магазинами, у которых уже есть позитивная репутация. При чем платежи должны быть верифицированы Visa, Mastercadr или 3D Secure…

Чтобы обезопасить себя от мошенников, эксперты советуют:

Не устанавливайте на компьютер и смартфон нелицензионные, взломанные программы…

Покупайте в сети только с помощью собственного компьютера или телефона, не производите покупки в общественных Wi-Fi сетях.

Установите защитное (антивирусное) программное обеспечение…

Если делаете покупки с помощью сайта, закройте другие вкладки на браузере…

"Ваша банковская карта заблокирована. Детали по номеру 093…", – рассылку с таким сообщением ежедневно получают тысячи украинцев. Если набрать указанный в СМС номер, собеседник попросит назвать номер карты и "номер оператора", который якобы указан на обратной стороне карты. Через считанные секунды на мобильный телефон придет еще одна СМС, уже с паролем от банка. Если озвучить его по телефону, можно лишиться всех денег на карте. Ежедневно сотни украинцев попадаются на "удочку мошенников" и доверчиво отвечают на все вопросы по телефону…

Вторая схема телефонных "банкиров" – обзвон потенциальных жертв. …Сразу же говорят о якобы заблокированной банковской карте, предлагают проверить, что же произошло. Или сообщают "о подозрительной деятельности" с картой. Главная цель – получить номер карты, срок ее действия и CVV-код. Этой информации достаточно, чтобы оплатить покупку в интернете, перевести средства с одной карты на другую с помощью онлайн-банкинга…

Еще одна популярная мошенническая схема – "я нашел ваш паспорт". Злоумышленники находят объявления о потерянном документе, звонят по указанному номеру телефона и соглашаются вернуть документ, но, например, за 500 грн. После они назначают место встречи и говорят, что документ принесет девушка, но она стеснительная и разговаривать не будет. Когда жертва уже ожидает на месте, раздается еще один телефонный звонок. Мошенник говорит, что в руки девушка брать деньги не хочет. Поэтому нужно подойти к терминалу, выбрать функцию "пополнить мобильный счет", внести 500 грн, но не нажимать "подтвердить". Якобы, как только принесут паспорт, можно будет сразу подтвердить операцию и забрать документ.

Как только жертва вносит указанную сумму в терминал, преступник прекращает разговор и перестает отвечать на мобильные звонки…» ***(Выяснилось, как воруют наличку с карт украинцев // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/228028-vyjasnilosj_kak_vorujut_nalichku_s_kart_ukraintsev). 23.03.2018).***

***

«Канада рішуче підтримує Україну, але не надаватиме країні допомогу у сфері кібербезпеки.

Про це йдеться у відповіді уряду Канади на звіт Постійного комітету федерального парламенту із питань оборони…

При цьому в уряді додали, що «Канада занепокоєна все більшим кібернетичним втручанням в Україну, в тому числі у важливу цивільну інфраструктуру, таку як електромережі».

В урядовій відповіді наголошується, що «Канада та її ключові союзники поділяють думку, що міжнародне законодавство повинно застосовуватися і в кіберпросторі, як у мирний, так і у військовий час».

«Канада також підтримує розробку добровільних міжнародних норм поведінки держав у кіберпросторі, особливо у мирний час», – зазначається у документі.

В оприлюдненому наприкінці грудня минулого року звіті Постійного комітету парламенту Канади з питань оборони «Канадська підтримка України у час кризи та збройного конфлікту», депутати закликають уряд відправити в Україну військовий персонал для допомоги у відбитті кібератак» ***(Канада занепокоєна кібербезпекою України, але допомагати не буде // Західна інформаційна корпорація(https://zik.ua/news/2018/03/31/kanada_zanepokoiena_kiberbezpekoyu_ukrainy_ale_dopomagaty_ne_bude_1296597). 31.03.2018).***

***

«21 марта правительственная команда реагирования на киберинциденты CERT-UA зафиксировала распространение в Украине банковского трояна Ursnif…

Данный вирус - Ursnif (или Gozi), который используется для кражи данных. Троян упакован и в процессе инициализации инфицирует процесс explorer.exe. В инфицированном коде пропущены некоторые части PE заголовка (MZ, PE) для усложнения анализа.

В CERT-UA рекомендуют организациям принять следующие меры:

– Ограничить возможности пользователей по установке и запуску нежелательных программных приложений для всех систем и служб. Ограничения этих привилегий может предотвратить запуск вредоносных программ;

– Обновить антивирусное программное обеспечение и запустить сканирование;

– Избегать сообщений указанного содержания и предостеречь персонал от запуска данных Javascript-файлов;

– Обеспечить мониторинг сетевого оборудования на факт обращения к подозрительным адресам…» ***(Владимир Кондрашов. В Украине под видом писем от НАПК опять распространяется опасный банковский вирус // Internetua (http://internetua.com/v-ukraine-pod-vidom-pisem-ot-nazk-opyat-rasprostranyaetsya-opasni-bankovskii-virus). 23.03.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Одним з напрямків міжнародної підтримки України має стати кібербезпека, однак Україна має ще поборотися за виділення коштів. Про це у ході Українсько-Литовського форуму інновацій в ІКТ для безпеки енергетичної інфраструктури заявив директор департаменту залучення інвестицій міністерства економічного розвитку та торгівлі Андрій Демчук…

"Литва виступали локомотивом плана Маршала для України, який передбачає надання 50 млрд євро протягом 10 років для фінансування проектів в Україні. Кібербезпека має стати одним із напрямків", - сказав він.

Як уточнив Демчук, міністерство провело низку зустрічей щодо плану Маршала з литовськими колегами…

…в Єврокомісії пообіцяли опрацьовати "план Маршала" для України в єдиний документ побудови дорожньої карти.» ***(Ася Красоха. МЕРТ про план Маршала: Україна, на думку донорів, демонструє низьку спроможність освоювати кошти // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1718939-mert-pro-plan-marshala-ukrayina-demonstruye-nizku-spromozhnist-osvoyuvati-koshti). 07.03.2018)***

***

«Поліцейські України та Великої Британії обговорили співпрацю у сфері кібербезпеки та боротьби з організованою злочинністю з огляду на збільшення кількості скоєння відповідних злочинів.

Як повідомляє прес-служба ГУ Нацполіції України, про це йшлося під час зустрічі в Лондоні глави Нацполіції Сергія Князєва з директором міжнародних відносин Національного агентства з питань боротьби зі злочинністю Великої Британії (NCA) Стівом Рейналдсом і керівником Департаменту з протидії кіберзлочинності Олівером Говером.

"С.Князєв і С.Рейналдс домовилися поглиблювати співробітництво між правоохоронним відомствами двох держав та підписати меморандум про співпрацю. Також учасники зустрічі обговорили взаємодію у протидії окремим видам злочинів", - інформують в українському правоохоронному відомстві…» ***(Правоохоронці Великої Британії та України домовилися поглиблювати співпрацю у протидії кіберзлочинності // Інтерфакс-Україна (http://ua.interfax.com.ua/news/general/490072.html). 06.03.2018).***

***

«Уряд Великої Британії занепокоєний тим, що Україну використовують як тестовий майданчик для кібератак та корупції з боку Російської Федерації. Про це заявив міністр внутрішніх справ Великої Британії з питань безпеки та боротьби з економічною злочинністю Бен Уоллс на зустрічі з українським колегою Арсеном Аваковим у Лондоні…

Він додав, що МВС Великої Британії зацікавлене в поглиблені співпраці з Міністерством внутрішніх справ України.

…Арсен Аваков наголосив, що МВС України і Національна поліція готові посилити співпрацю з поліцією Великої Британії за всіма напрямами кримінального блоку…» ***(Україну використовують як тестовий майданчик для кібератак, - МВС Британії // Громадське радіо (https://hromadskeradio.org/news/2018/03/06/ukrayinu-vykorystovuyut-yak-testovyy-maydanchyk-dlya-kiberatak-mvs-brytaniyi). 06.03.2018).***

***

«В ходе своего официального визита в Государство Израиль президент Болгарии Румен Радев (Rumen Radev) счел нужным обсудить также и перспективы сотрудничества двух стран в области обеспечения кибернетической безопасности.

Среди прочего, болгарский президент посетил Национальный компьютерный центр экстренного реагирования в Беэр-Шеве, в ходе экскурсии по которому иностранного гостя сопровождал Игаль Унна (Yigal Unna), рассказавший Радеву о работе и функциях центра, а также о его взаимодействии с другими такими объектами, занятыми обеспечением безопасности…» ***(Болгария хочет сотрудничать с Израилем в сфере кибербезопасности // ISRAland Online Ltd. (http://www.isra.com/news/212976). 22.03.2018).***

***

Світові тенденції в галузі кібербезпеки

«Проблема кибербезопасности является главной угрозой для роста мирового бизнеса. Это следует из данных Глобального опроса инвесторов за 2018 год, проведенного компанией PwC…

В частности, 41% инвесторов назвали кибератаки самой серьезной угрозой для бизнеса…

При этом по мнению руководителей компаний, кибератаки занимают только третье место среди самых серьезных рисков для бизнеса — такое мнение высказали 40% респондентов. Среди главных угроз они выделили терроризм и чрезмерное регулирование - 41% и 42% соответственно.

Опрос проведен среди 1293 руководителей компаний и 663 специалистов в области инвестиций из разных стран мира» ***(Инвесторы назвали самую серьезную угрозу бизнесу // «Парламентская газета» (https://www.pnp.ru/economics/investory-nazvali-samuyu-sereznuyu-ugrozu-biznesu.html). 01.03.2018).***

***

«…Как показало исследование «Защита виртуальной инфраструктуры», проведенное компанией «Код безопасности», особо остро это ощущают малые компании: представители 66% из них отметили, что боятся действий администратора виртуальной инфраструктуры. Эти опасения подтвердили и их коллеги из средних (65%) и крупных компаний (55%)...

Респонденты отметили, что в виртуальных инфраструктурах(ВИ) хранят и обрабатывают общедоступную информацию (76%), конфиденциальные данные (70%) и сведения, составляющие государственную тайну (3%)…

В ходе исследования аналитиками «Кода безопасности» угрозы при использовании виртуальной инфраструктуры были объединены в следующие группы:

Уязвимости ПО гипервизора

Нарушение процедуры аутентификации

Недоступность ресурсов ВИ

Ошибки архитектуры ВИ

Несанкционированный доступ

Внутри каждой группы угроз была произведена оценка их критичности. Самой многочисленной стала группа угроз несанкционированного доступа.

Риск выхода из строя критичных систем и потери данных побуждает бизнес внимательно подходить к обеспечению защиты виртуальной инфраструктуры. При создании системы защиты ВИ респонденты выделили в числе трех важнейших задач резервное копирование виртуальных машин, антивирусную защиту и мониторинг событий безопасности ВИ.

…результаты исследования позволяют сделать вывод о том, что …защиты сегодня требует сама виртуальная среда (причем от действий не только злоумышленника, но и собственного администратора)…

Большинство респондентов «Кода безопасности» сходятся во мнении, что предотвратить риски и снизить критичность угроз в виртуальных средах поможет комплексный и системный подход к безопасности виртуальной инфраструктуры…

По мнению опрошенных специалистов, в число приоритетных требований при выборе решения для защиты виртуальной инфраструктуры входят:

- отсутствие высокой нагрузки на виртуальную инфраструктуру;
- низкие требования к ресурсам виртуализации;
- простота настройки и эксплуатации;
- отсутствие необходимости переконфигурирования ВИ;
- надежность и стабильность работы;
- поддержка современных платформ виртуализации;
- соответствие требованиям регулирующих органов»

(Главная опасность виртуализации – администратор // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5480991-Glavnaya-opasnost-virtualizacii-adm.html#ixzz5AC3xqwRO). 16.03.2018).

***

«…В ходе исследования, проведенного в конце 2017 года агентством Vanson Bourne по заказу Cloud Industry Forum CIF, было опрошено 200 руководителей ИТ-подразделений предприятий из разных стран, в которых работает более 500 человек. 89% опрошенных считают, что унаследованная технология (legacy technologies) является препятствием для успешной цифровой трансформации их компаний.

Главной причиной этой проблемы респонденты называли риск прерывания главных бизнес-процессов при любом изменении унаследованной системы (46%) и большие расходы на ее изменение (40%). Кроме того, 30% ответили, что у них не хватает обученного персонала для обслуживания унаследованной инфраструктуры, а 27% указали на отсутствие четкого плана миграции бизнес-критичных приложений.

Комментируя результаты исследования, исполнительный директор российского отделения TmaxSoft Андрей Рева сказал: «Проблемы унаследованных технологий хорошо известны и с ними сталкиваются практически все компании.

Подавляющее большинство предприятий ранее инвестировали значительные средства в ИТ и поэтому не могут начать свою цифровую трансформацию с чистого листа. Очевидно, что унаследованные технологии превратились в критически важную для бизнеса проблему, поскольку во многих компаниях ИТ-инфраструктура по-прежнему построена на платформе мэйнфреймов. Унаследованная архитектура мэйнфреймов не способна удовлетворить новые потребности экономики эры цифровой трансформации, что создает серьезные проблемы для тех компаний, которые хотят сохранить конкурентоспособность и динамичность…» ***(Названа главная угроза цифровой трансформации бизнеса // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5485382-Nazvana-glavnaya-ugroza-cifrovoj.html#ixzz5AC4Y8KzS). 19.03.2018).***

***

«…Исследователи безопасности из компаний Qrator Labs и «Валарм» опубликовали отчет об основных тенденциях и проблемах в области кибербезопасности интернет-ресурсов в 2017 году. Основными причинами инцидентов являются риски, связанные с человеческим фактором, основанные на недостаточной автоматизации процессов, следует из совместного доклада компаний.

Как отметили специалисты, одной из основных проблем безопасности в 2017 году стал массовый взлом IoT-устройств и облачных сервисов…

Помимо этого, возросло количество инцидентов маршрутизации. По словам экспертов, атаки данного типа могут угрожать целым экосистемам, использующим взаимосвязанные части инфраструктуры…

Исследователи также отметили рост количества инцидентов, связанных с человеческими ошибками. В частности, речь идет об утечках данных о клиентах Uber и Equifax .

Кроме того, в 2017 году наблюдался резкий скачок интереса хакеров к различным криптовалютам, а именно к кампаниям по первичному размещению монет (initial coin offering, ICO)…» ***(Названы главные проблемы безопасности web-ресурсов в 2017 году // SecurityLabRu (https://www.securitylab.ru/news/492191.php). 19.03.2018).***

***

«…Представлена новая версия руководства по кибербезопасности CIS Controls Version 7, включающая в себя 20 рекомендаций по защите информационных технологий.

…В частности, был изменен приоритет некоторых рекомендаций (рекомендации в руководстве отсортированы по степени важности) для того, чтобы лучше отражать текущую ситуацию в мире киберугроз.

Помимо этого, все рекомендации в CIS Controls V7 были разделены на 3 категории: базовые, основополагающие и организационные…

Рекомендации CIS Controls обеспечивают четкое, приоритетное руководство, помогающее организациям решать самые распространенные проблемы в сфере

киберугроз» ***(Опубликована 7 версия рекомендаций CIS Controls // SecurityLabRu (https://www.securitylab.ru/news/492247.php). 22.03.2018).***

***

«Объем рынка средств информационной безопасности по итогам 2017 г. достиг $31 млрд, продемонстрировав годовой рост на 10%. Из этой суммы $4 млрд приходится на сегмент «безопасности как услуги» (SaaS), что на 21% больше аналогичного показателя за предыдущий год.

Такие данные приводит CNews со ссылкой на исследование, проведенное компанией Canalys.

Траты на SaaS растут быстрее, чем траты на традиционное защитное ПО и аппаратуру — эти сегменты продемонстрировали годовой рост на 5% и 10% соответственно, в совокупности достигнув $27 млрд.

Согласно прогнозу Canalys, в 2018-2019 гг. SaaS продолжит расти, однако большая часть средств по-прежнему будет тратиться на аппаратуру и традиционное ПО, причем эти сегменты также продолжат рост.

Стремительный рост рынка SaaS, по словам аналитика Canalys Клаудио Станке (Claudio Stahnke), объясняется тем, что такие решения являются более гибкими по сравнению с традиционной моделью лицензирования ПО…

Такие игроки рынка кибербезопасности как Cisco, McAfee и Trend Micro расширили в прошлом году ассортимент облачных продуктов, причем функционал этих продуктов уже практически не отличается от того, который присутствует в лицензионных версиях…

Весь мировой рынок корпоративной информационной безопасности по итогам 2017 г. исследовательская компания Gartner оценивает в $89,13 млрд — на $7 млрд больше, чем в предыдущем году.

Из них, по данным компании, более $53 млрд было потрачено на ИБ-услуги, еще $16,2 млрд — на решения для защиты инфраструктуры, и $10,93 млрд — на оборудование для сетевой безопасности. Кроме того, $4,64 млрд пошло на потребительское ПО, и $4,3 млрд — на системы идентификации и управления доступом…» ***(«Безопасность как услуга» растет колоссальными темпами, обгоняя «обычное» ПО и «железо» // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5486889-Bezopasnost-kak-usluga-rastet-kolos.html#ixzz5As997Qc7). 26.03.2018).***

***

«…Компания Netwrix – международный разработчик решений для аудита изменений в IT-инфраструктуре, провела анализ рынка и выделила пять ключевых тенденций информационной безопасности, которые влияют на стратегии безопасности компаний в 2018 году, а также на развитие IT-рынка в целом…

1. Blockchain – “цепочка блоков”. Технология Blockchain позволяет хранить данные децентрализованным и распределенным образом, что исключает единую точку отказа и предотвращает доступ злоумышленников к большому объему данных…

2. Фокус на внутренних угрозах. Исследование Netwrix IT Risks Report показало, что в большинстве организаций не осуществляется контроль за действиями пользователей, что делает их инфраструктуры уязвимыми для инсайдерских угроз

3. Непрерывная оценка рисков. Gartner предлагает использовать подход CARTA в оценке рисков. Данный подход рассматривает безопасность как непрерывный процесс, который постоянно меняется и должен регулярно пересматриваться…

4. Расширенная аналитика. Поскольку программное обеспечение для ИБ генерирует большие объемы данных – необходима развернутая и детальная аналитика всей собранной информации, чтобы оценить все события в системе и риски…

5. Индивидуальный подход к выбору ИБ решений. Компании больше не готовы внедрять стандартные ИБ решения. Им требуются продукты, подходящие под их инфраструктуру, задачи и бюджет…» ***(Топ 5 тенденций кибербезопасности 2018 года // Сервис размещения пресс-релизов (http://pr.adcontext.net/18/03/27/273063). 27.03.2018).***

***

«Мировые расходы на решения для обеспечения информационной безопасности (ИБ), включая оборудование, ПО и сервисы, в 2018 году увеличатся на 10,2% и достигнут 91,4 млрд долларов США, прогнозируют аналитики IDC. Специалисты полагают, что в условиях усиливающейся регуляторной нагрузки и растущего числа киберугроз подъем на рынке ИБ-технологий продолжится. Ожидается, что к 2021 году глобальные расходы на соответствующие технологии достигнут 120,7 млрд долларов, с учетом чего показатель среднегодового роста (CAGR) в период с 2016 по 2021 составит 10%.

…Самые щедрые отрасли с точки зрения затрат на ИБ-решения — банковский сектор, дискретное производство и федеральное/центральное правительство — в 2018 году израсходуют более 27 млрд долларов. Четыре другие отрасли (процессное производство, сфера профессиональных услуг, потребительский сектор и телекоммуникации) потратят на информационную безопасность более 5 млрд долларов каждая…

С географической точки зрения ведущим рынком решений для обеспечения кибербезопасности будут США, где затраты на ИБ-решения в 2018 году достигнут 38 млрд долларов. Также пятерку лидеров войдут Великобритания (6,5 млрд долларов), Китай (6 млрд долларов), Япония (5,1 млрд долларов) и Германия (4,6 млрд долларов)» ***(Мировые расходы на ИБ-технологии в 2018 году достигнут 91,4 млрд долларов // Goodnews.ua (http://goodnews.ua/technologies/mirovye-rasxody-na-ib-texnologii-v-2018-godu-dostignut-914-mlrd-dollarov/). 31.03.2018).***

***

Сполучені Штати Америки

«Спецпрокурор США Роберт Мюллер, який проводить розслідування у зв'язку з втручанням РФ в американські президентські вибори, може висунути нові звинувачення росіянам під приводом того, що вони нібито викрали інформацію у Демократичної партії під час американської передвиборчої гонки 2016 року…

За версією джерел телеканалу NBC з числа офіційних осіб, апарат Мюллера має намір пред'явити звинувачення на основі секретних матеріалів, зібраних ЦРУ, ФБР, Агентством національної безпеки і Міністерством внутрішньої безпеки.

За твердженням телеканалу, у спецпрокурора вже протягом деякого часу були "докази, достатні для порушення справи", однак "час для цього може бути обумовлено стратегічними міркуваннями".

Очікується, що це відбудеться в "наступні тижні або місяці", однак не виключається, що Мюллер може і відмовитися від даних планів…» ***(Самуїл Проскуряков. NBC: Мюллер може висунути нові звинувачення росіянам через кібератаки // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1718031-nbc-myuller-mozhe-visunuti-novi-zvinuvachennya-rosiyanam-cherez-kiberataki). 02.03.2018).***

***

«…Компания Facebook оказалась в центре очередного большого скандала, связанного с утечкой персональных данных. В скандале также оказалась замешена британская компания Cambridge Analytica…

За несколько лет до этого Cambridge Analytica участвовала в совместном проекте с профессором университета Кембриджа Александром Коганом. Он разработал приложение, получившее название thisisyourdigitallife и предназначенное для "исследовательских целей" – приложение могло делать предсказания на основе анализа личностных черт, … которое для своей работы должно было получить доступ к пользовательским данным.

Несколькими днями ранее Facebook признал, что приложение установили 270 тысяч человек, предоставив его создателям доступ к своему местоположению. Однако данные пользователей оказались доступны не только непосредственному разработчику, но и компании Cambridge Analytica, что нарушило запрет соцсети на передачу данных третьим лицам. Когда в Facebook узнали об этом нарушении, приложение было немедленно удалено, а все вовлечённые в инцидент стороны заявили о том, что они уничтожили полученные ими персональные данные пользователей. Однако, как недавно выяснилось, далеко не все данные были удалены. Более того, приложение получало доступ к информации друзей пользователя, установившего его (в случае если такая возможность не была отключена в настройках приватности). В итоге в распоряжении Cambridge Analytica оказались персональные данные порядка 50 миллионов человек…

Этот скандал уже причинил Facebook серьезный репутационный ущерб… Генеральный прокурор штата Массачусетс Мора Хили объявила в субботу о начале расследования против обоих компаний…» ***(Максим Волков. Очередной скандал с утечкой персональных данных сильно ударил по Facebook // РосКомСвобода (https://roskomsvoboda.org/37210/). 20.03.2018).***

***

«…Национальный институт стандартов и технологий США (NIST) опубликовал вторую часть руководства по кибербезопасности для предприятий и организаций NIST Special Publication 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems.

Документ содержит перечень рекомендаций по противостоянию различным типам киберугроз.

«Данная публикация посвящена организации киберустойчивости, которая тесно связана с безопасностью и отказоустойчивостью. Киберустойчивость - это способность предвидеть, выдержать, восстановиться и адаптироваться к неблагоприятным условиям, атакам или компрометации систем, которые используют или активируют различные компоненты независимо от их источника», - следует из руководства.

Помимо этого, во второй части руководства рассматриваются действия по разработке систем, способных противостоять кибератакам и при этом сохранять работоспособность…» ***(NIST опубликовал 2 часть руководства по кибербезопасности // SecurityLabRu (https://www.securitylab.ru/news/492262.php). 23.03.2018).***

***

Країни ЄС

«…В Центральной Европе сейчас происходит что-то странное: часы отстают, и не на доли секунды, а на целые минуты. Действительно ли в этом виноваты майнеры?..

С середины января у Европейской континентальной энергетической системы происходят значительные аномалии. По данным Европейской сети системных операторов передачи электроэнергии, у 25 стран, от Испании до Турции и от Польши до Нидерландов, наблюдалось "отклонение частоты системы от среднего значения в 50 Гц". Обнаружили и месторасположение неисправности – Косово и Сербия. Причина пока не известна…

Отклонения вызвали замедление работы часов, использующих частоту энергетической сети. В результате время отстает на 6 минут. Неясно, как именно проявляется это замедление, в течение какого периода, и можно ли вручную отрегулировать часы. Понятно одно – нехватка электроэнергии огромна: 113 ГВтч, что равно потреблению электроэнергии в Гренландии в течение полугода…

Вопрос, что может стать причиной такой огромной нехватки электроэнергии, остается открытым. Это может быть секретный проект наподобие Большого адронного коллайдера, правительственная ошибка или майнинг криптовалют. Большинство подозрений падает на последний вариант. Электричество в Сербии и Косово – одно из самых дешевых в Европе, при этом стоимость майнинга биткоина в этих регионах оценивается в 3 133 долларов...» ***(Ирина Фоменко. В Европе отстают часы, а обвиняют в этом майнеров // Internetua***

(http://internetua.com/v-evrope-otstauat-csas-a-obvinyauat-v-etom-mainerov). 10.03.2018).

***

«…Виконуючий обов'язки міністра внутрішніх справ Німеччини Томас де Мезьєр заявив 1 березня, що хакерську атака на урядову мережу країни слід сприймати дуже серйозно. За його словами, втручання хакерів було заздалегідь спланованим та технічно здійснене на високому рівні…

Утім, за словами глави МВС ФРН, цей випадок не заперечує факту, що кібербезпека в Німеччині перебуває на високому рівні, а урядова мережа є однією з найбільш захищених у світі… Він запевнив, що атаку було ізольовано та взято під контроль, за високопрофесійними нападниками велося спостереження, аби з'ясувати їхні цілі та вжити відповідних заходів безпеки в урядовій мережі.

Тим часом голова комісії Бундестагу з контролю за діяльністю спецслужб Армін Шустер заявив, що хакерська атака, вочевидь, досі триває…» ***(Самуїл Проскуряков. Глава МВС Німеччини визнав серйозність хакерської атаки на урядову мережу // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1718025-glava-mvs-nimechchini-viznav-seryoznist-khakerskoyi-ataki-na-uryadovu-merezhu). 02.03.2018).***

***

«…Служба загальної розвідки та безпеки Нідерландів (AIVD) відзначила у своєму звіті за 2017 рік, що все більша кількість іноземних держав використовують кібершпигунство "для отримання інформації, яку вони застосовують для геополітичної вигоди".

У звіті підкреслюється роль Росії, яка надзвичайно включена "у прихований цифровий вплив на політичні процеси прийняття рішень". Аналогічні спроби спостерігалися з боку Китаю.

У доповіді агентство також повідомило, що онлайн-шпигунство використовується для проникнення в європейські транснаціональні корпорації, дослідні інститути, а також у енергетичний, технологічний і хімічний сектори…» ***(Розвідка Нідерландів: обсяг і складність кібератак в Європі зростають // Європейська правда (http://www.eurointegration.com.ua/news/2018/03/6/7078442/).05.03.2018).***

***

«…Посольство официально запросило у МИД Великобритании объяснений относительно угроз осуществить кибератаку, звучавших в парламенте и в СМИ. Россия очень серьёзно относится к нарушениям в сфере кибербезопасности», — говорится в сообщении дипломатического ведомства в сети микроблогов Twitter.

Ранее во вторник российское посольство в Лондоне также попросило Соединённое Королевство взвесить все последствия возможной кибератаки на Россию, о которой заявили в британском парламенте.

В понедельник, 12 марта, премьер-министр Великобритании Тереза Мэй заявила, что Скрипаль и его дочь отравили разработанным в России нервно-

паралитическим веществом под названием «Новичок». Она также выдвинула ультиматум, по которому Москва в срок до вечера 13 марта должна предоставить подробные объяснения по этой теме. В противном случае глава британского правительства пригрозила принять серьёзные меры в отношении РФ.

Ранее во вторник министр иностранных дел России Сергей Лавров опроверг любые предположения об участии российских представителей в деле об отравлении Скрипаля…» ***(Жанна Звягина. РФ официально запросила у Великобритании объяснений в связи с угрозами кибератаки // «Парламентская газета» (https://www.pnp.ru/politics/rf-oficialno-zaprosila-u-velikobritanii-obyasneniy-v-svyazi-s-ugrozami-kiberataki.html). 14.03.2018).***

***

Китай

«…В последние годы китайские специалисты по кибербезопасности занимали лидирующие позиции на всех хакерских соревнованиях, однако теперь этому пришел конец. Правительство КНР запретило отечественным ИБ-экспертам участвовать в международных соревнованиях из соображений национальной безопасности...

По словам представителей пекинской ИБ-компании Beijing Chaitin Technology, в конце прошлого года власти запретили им участвовать в подобных соревнованиях. Теперь главными приоритетами компании будут улучшение продуктов и «обеспечение безопасности киберпространства в Китае».

В течение долгих лет кибератаки являются камнем преткновения в отношениях между США и КНР. Решение отказаться от участия в соревнованиях «белых» хакеров, помогающих таким компаниям, как Apple и Microsoft улучшать безопасность своих продуктов, было принято на фоне возрастающего напряжения между двумя государствами…

В прошлом году китайская команда, включавшая в себя специалистов из Qihoo 360, Tencent и Beijing Chaitin Technology, стала безусловным фаворитом соревнований Pwn2Own в Ванкувере. В нынешнем году после постановления правительства команда не принимала участия в соревнованиях» ***(Китай запретил своим ИБ-экспертам участвовать в хакерских соревнованиях // SecurityLabRu (https://www.securitylab.ru/news/492248.php). 22.03.2018).***

***

Російська Федерація та країни

«Вашингтон под надуманным предлогом буквально за час до начала сорвал консультации с Москвой по кибербезопасности в Женеве, заявил замглавы МИД Сергей Рябков…

По словам дипломата, «эти консультации должны были состояться в Женеве 27-28 февраля».

«Буквально за час до запланированного их начала, когда российская межведомственная делегация уже была на место, из госдепартамента нас уведомили о решении администрации отказаться от проведения встречи – опять с абсолютно надуманной необоснованной ссылкой на некие «дестабилизирующее действия России в электронном пространстве», – добавил замглавы МИД…» ***(Алина Назарова. США сорвали консультации с Россией по кибербезопасности // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/3/5/911085.html). 05.03.2018).***

***

«Замглавы Госдепа Томас Шэннон прокомментировал ситуацию вокруг сорвавшихся по вине США переговоров с Россией в Вене по вопросу стратегической стабильности…

По словам замглавы Госдепа, американская сторона «абсолютно открыта для переноса переговоров» и хочет услышать предложения «российских друзей», чтобы встреча все же состоялась.

Он не стал называть дату, которая устроила бы американцев, и предложил «подождать» замглаву МИД России Сергея Рябкова…» ***(Антон Антонов. США прокомментировали срыв переговоров с «российскими друзьями» // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/3/8/911644.html). 08.03.2018).***

***

«Из США осуществляется до 28% кибератак против России, заявил руководитель Временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела России Андрей Климов в прямом эфире телеканала «Россия 24»…

«Каждый год мы фиксируем кратное увеличение кибератак в отношении России. Это не фейк. Это подтверждали эксперты ООН. К выборам это всё больше усиливается, атаки на наши важные системы составляют сотни тысяч в сутки. 25-28% этих атак исходят с территории США», — сказал он…» ***(Климов: из США осуществляется до 28% кибератак против России // «Парламентская газета» (https://www.pnp.ru/politics/klimov-iz-ssha-osushhestvlyaetsya-do-28-kiberatak-protiv-rossii.html). 06.03.2018).***

***

«До 200 тысяч кибератак могут обрушиться на открытую часть интернет-платформ ЦИК РФ в день выборов президента 18 марта. Об этом заявил 7 марта глава Временной комиссии Совета Федерации по защите госсуверенитета и предотвращению вмешательства во внутренние дела России Андрей Климов в Общественной палате.

Он принял участие в совместном заседании временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела Российской Федерации и Комиссии ОП РФ по

безопасности и взаимодействию с ОНК на тему «Идеологические войны против России. Меры и пути противодействия»…

По его словам, сегодня основная проблема также исходит не от органов госпропаганды США, а от НКО и общественных организаций из-за рубежа. …Он напомнил, что 28 февраля представил на пленарном заседании Совета Федерации открытую часть текста доклада о работе Комиссии, а 5 марта на расширенном заседании Комиссии прошло очень горячее обсуждение документа, который состоит из 82 страниц.

…Доклад, о котором говорил Климов, представляет работу Комиссии с июня 2017 года по февраль 2018 года.

Чуть позже комиссия подготовит специальный доклад, посвящённый попыткам зарубежного вмешательства в выборы Президента РФ в 2018 году, который планирует опубликовать во второй половине 2018 года. В июле нынешнего года будет начата публикация чёрной книги вмешательства в дела суверенных государств…» ***(Андрей Климов. Климов спрогнозировал сотни тысяч кибератак на открытые платформы ЦИК // «Парламентская газета» (https://www.pnp.ru/politics/klimov-sprognoziroval-sotni-tysyach-kiberatak-na-otkrytye-platformy-cik.html). 07.03.2018).***

***

«…В день голосования, 18 марта 2018 горда, председатель ЦИК Элла Памфилова заявила, что в ночь перед выборами Президента РФ сайт комиссии подвергся DDOS-атаке из 15 стран…

Позднее секретарь ЦИК Майя Гришина сообщила, что кибератака была зарегистрирована и на информационно-справочный центр комиссии…

Накануне выборов об увеличении хакерской активности и кибератак на российские сайты сообщал также глава Минкомсвязи Николай Никифоров... Никифоров добавил, что ведомство уверено в работоспособности систем защиты…

Президент «Ростелекома» Михаил Осеевский на церемонии старта голосования на выборах президента РФ в ЦИКе отмечал, что 17-го марта в субботу, — в «день тишины», — сайт Роскомнадзора подвергся хакерской атаке…

Затем, уже в день голосования 18 марта, Михаил Осеевский заявил, что в ходе выборов порталы видеотрансляции и ЦИКа подвергались десяткам хакерских атак…

Осеевский отметил, что пока не будет раскрывать подробности и говорить, откуда были совершены атаки…

Уже вечером в воскресенье глава Минкомсвязи Никифоров заявил, что «…никакого влияния ни на процедуру трансляции, ни на тем более на систему ГАС «Выборы» такие атаки влияния оказать не смогли».

Однако слова Никифорова опровергаются результатами вчерашнего онлайн-тестирования исследовательского центра Citizen Lab, University of Toronto, о чём сообщила представитель лаборатории Ксения Ермошина в своём Telegram-канале.

Как оказалось, официальный сайт видеотрансляции выборов Nashvybor весь день был недоступен за пределами России, то есть за выборами невозможно было наблюдать онлайн в целом большинстве стран…

Точно также видеотрансляции были недоступны и для россиян, которые заходят в интернет посредством VPN. То есть доступ на сам сайт Nashvybor2018 для заграничных и анонимных пользователей не ограничивался, а вот трансляция почему-то блокировалась. Сотрудниками РосКомСвободы также была проведена проверка, и действительно — при включённом VPN увидеть трансляцию под американским, сингапурским, нидерландским или британским IP было невозможно…

ЦИК заранее предупреждал о том что сайт Nashvybor будет недоступен с зарубежных IP. Однако российские «власти» не предоставили внятных причин по которым следует ограничить доступ к видеотрансляциям с избирательных участков для жителей других стран...» ***(Миру закрыли возможность наблюдать за выборами в целях защиты от кибератак // РосКомСвобода (https://roskomsvoboda.org/37183/). 19.03.2018).***

***

«Росія ніколи не екстрадує своїх громадян, яких Сполучені Штати звинувачують у хакерських атаках під час виборчої кампанії у 2016 році.

Про це президент РФ Володимир Путін заявив в інтерв'ю телеканалу NBC…

Сполучені Штати почали розслідувати втручання Росії у вибори президента 2016 року після того, як радник кампанії Трампа проговорився австралійському дипломату.

На слуханнях у Комітеті з розвідки колишній секретар Департаменту внутрішньої безпеки США Джей Джонсон заявив, що замовником хакерських атак під час виборів президента у 2016 році був особисто Путін…» ***(Марія Леонова. Путін про кібератаки під час виборів США: Росія ніколи не екстрадує своїх громадян // громадське телебачення (https://hromadske.ua/posts/putin-pro-kiberataky-pid-chas-vyboriv-ssha-rosiia-nikoly-ne-ekstraduie-svoikh-hromadian). 04.03.2018).***

***

«Количество хакерских атак на информационные объекты России, в том числе атак, направленных на компрометацию учетных данных, увеличилось в 2017 году более чем в четыре раза, сообщили в центре «Антистихия»…

По данным центра, больше всего атак приходилось на вирусы-шифровальщики (36%), эксплуатацию уязвимостей (26%), а также компроментацию учетных данных (23%).

При этом в общем количестве хакерских атак в России DDos-атаки занимают 8%, а манипулирование, взломы СМИ и социальных медиаресурсов – 6%.

Российские спецслужбы отметили возросшую активность иностранных разведок, пытающихся внедрить вредоносное ПО в информационные системы госорганов страны…

При этом российские ресурсы оказались в большинстве случаев защищены недостаточно, что было вызвано низкой осведомленностью пользователей, отсутствием квалификации у персонала и некачественным доступом в интернет…» ***(Дмитрий Зубарев. Число хакерских атак на российские объекты значительно***

выросло // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/3/14/912332.html). 14.03.2018).

***

«…Различные российские силовые управления закупают программы израильской компании Cellebrite, недавно объявившей о взломе последней модели iPhone. Как утверждает производитель, после обхода блокировки эти устройства позволяют скачивать информацию со смартфонов — фото, историю звонков, переписку, в том числе в популярном мессенджере Telegram…

О том, что российские силовики заинтересовались данной техникой и ПО, стало известно из публикаций на сайте госзакупок.

В частности, управление Следственного комитета по Волгоградской области приобрело за 800 тысяч рублей комплекс UFED Touch2 для автономного съема информации, производимый Cellebrite. Управление МВД по Хабаровскому краю за 1,2 миллиона рублей закупало обновление программного обеспечения для исследования мобильных устройств UFED Touch.

В 2016 глава Следственного комитета РФ Александр Бастрыкин официально подтвердил, что ведомство использует решения израильской компании…

Кроме того, оборудование Cellebrite приобретал Сбербанк. В пресс-службе банка заявили, что оно используется для борьбы с вирусами на устройствах с операционной системой Android…» ***(Российские силовики планируют взламывать iPhone израильским ПО // РосКомСвобода (https://roskomsvoboda.org/37080/). 14.03.2018).***

***

Інші країни

«Тамир Пардо (Tamir Pardo), в прошлом глава Моссада, политической разведки Израиля, которая по своему назначению и функциям сравнима с ЦРУ, создал компанию XM Cyber, куда пригласил специалистов в области кибербезопасности.

В итоге Пардо удалось переманить специалистов, работавших в командах израильских служб безопасности, среди которых Моссад, Шабак или (Шин-бет) и элитное подразделение армии 8200. …Пардо пришел к тому, что необходимо создать новые методы имитации кибератак, благодаря чему была запущена соответствующая платформа. «Мы создали машину, которая будет выполнять работу, которую раньше выполняли специалисты», — утверждает Пардо…» ***(Олег Иванов. Бывший глава Моссада переманил кибербезопасников из спецслужб // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-03-21-1447/25780). 21.03.2018).***

***

«Войска территориальной обороны» Польши продолжают формироваться, сейчас в их составе числится около 7 тыс. человек, но к 2019 году это число будет доведено до 50 тыс…

…помимо обычных задач по защите ключевых объектов инфраструктуры и обеспечения безопасности военных целей так называемые войска территориальной обороны будут противодействовать дезинформации, отражать кибератаки, поддерживать патриотические идеалы. Кроме того, именно эти «войска» будут регулировать ситуацию в условиях кризиса или военного положения…» ***(Ольга Никитина. NI рассказал о создаваемых для противостояния с Россией польских войсках // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/3/5/911027.html). 05.03.2018).***

***

«…Совет ЕС во вторник, 6 марта, дал старт 17 общим проектам в сфере безопасности. Речь идет о проектах в рамках инициативы PESCO (Permanent Structured Cooperation) - постоянного структурного сотрудничества, механизм которого ЕС запустил в декабре 2017 года.

…Участие в PESCO является добровольным - из 28 стран-членов ЕС к нему присоединились 25 (кроме Великобритании, Дании и Мальты). …государства-участники взяли на себя 20 обязательств, например, регулярно повышать оборонные бюджеты.

Другим обязательством является участие в общих проектах, которые и составляют практическую часть PESCO. Каждый из проектов ведет одна страна, задействованы в нем будут лишь те из 25 государств, которые сами того пожелают…

Проекты PESCO двух типов: совместные учения и повышение операционной готовности, а также создание новых образцов вооружений и техники…

Однако эти проекты касаются не только обороны, но и безопасности в целом. Так, Литва инициировала проект создания групп быстрого реагирования в сфере кибербезопасности. Они должны будут помогать преодолевать последствия кибератак на компьютерные сети как военного значения, так и других госорганов, а также на гражданскую инфраструктуру…

Хотя проекты в рамках PESCO стартовали только сейчас, подготовительная работа по многим из них уже ведется. В проекте, который инициировала Литва, принимают участие семь стран - Испания, Нидерланды, Румыния, Финляндия, Франция и Хорватия. Германия является наблюдателем. На этот год его участники ставят две главные цели. Первая - проанализировать законодательство, понять, насколько оно позволяет странам помогать друг другу в вопросах кибербезопасности. Вторая - создать первую группу и опробовать ее на практике…

…смысл проекта состоит в том, что, предоставляя одного сотрудника в команду быстрого реагирования, каждая страна-участник сможет воспользоваться в случае необходимости группой из, допустим, семи экспертов. Это особенно важно во время мощных кибератак. Хотя первая линия защиты - это национальные

структуры, но в критических ситуациях недостаток персонала ощущается особо остро. Кроме того, каждый из членов группы быстрого реагирования будет иметь свою специализацию.

Сначала планируется, что помощь будут получать страны-участники проекта… Однако по мере развития проекта говорят литовцы, возможна помощь и другим странам, даже не входящим в ЕС.

Замминистра обороны Литвы Эдвинас Керза заявил, что если кибератака на компьютерные сети Украины сейчас повторится, и Киев обратиться за помощью, то на данный момент непонятно, что можно сделать. Потому Литва и хотела бы создать законодательные рамки, чтобы "команда быстрого реагирования могла сесть на самолет, прилететь в Украину, применить свои инструменты и практически защитить электросети".

Ожидать быстрых результатов от проектов в рамках PESCO не следует. Во вторник Совет ЕС утвердил рекомендацию касательно дорожной карты постоянного структурного сотрудничества. Лишь в июне планируется принять правила управления проектами, а до января 2019 года страны-участницы должны представить свои национальные планы реализации PESCO…» ***(Юрий Шейко . Как Литва будет помогать Евросоюзу защищаться от кибератак // Deutsche Welle (http://www.dw.com/ru/%D0%BA%D0%B0%D0%BA-%D0%BB%D0%B8%D1%82%D0%B2%D0%B0-%D0%B1%D1%83%D0%B4%D0%B5%D1%82-%D0%BF%D0%BE%D0%BC%D0%BE%D0%B3%D0%B0%D1%82%D1%8C-%D0%B5%D0%B2%D1%80%D0%BE%D1%81%D0%BE%D1%8E%D0%B7%D1%83-%D0%B7%D0%B0%D1%89%D0%B8%D1%89%D0%B0%D1%82%D1%8C%D1%81%D1%8F-%D0%BE%D1%82-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA/a-42851802?maca=rus-rss-MetaUA_rus_V_Mire-3045-xml-mrss). 07.03.2018).***

***

«…Экс-помощник госсекретаря США по делам Европы и Евразии и бывший официальный представитель Госдепа Виктория Нуланд рассказала о планах ответить Москве на предполагаемое вмешательство в выборы президента США. Предложения об ответном вмешательстве разрабатывали координатор Белого дома по кибербезопасности Майкл Дэниел и эксперт по РФ в совете национальной безопасности Селеста Уолландер, которая работала над этим вместе с Нуланд, сообщил интернет-портал Yahoo.com 9 марта.

Об этом пишут авторы книги "Русская рулетка: инсайдерская история о войне Путина против Америки и избрании Дональда Трампа" ("Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump"), которая выйдет в продажу 13 марта, — журналист Yahoo Майкл Исикоф и главный редактор журнал Mother Jones Дэвид Корн…

…В числе предложений были также кибератаки на российские разведведомства и кибератака Агентства национальной безопасности, которая бы

разоблачила созданные Москвой сайты и российских хакеров Guccifer 2.0 и DCLeaks, причастных к обнародованию документов Демократической партии.

Вашингтон отказался от планов ответного кибердара

Однако в Белом доме решили не отвечать России на возможное вмешательство. Советники Обамы по внутренней безопасности Сьюзан Райс и Лайза Монако посчитали, что если информация о подготовке ответа просочится в СМИ, то Обама окажется "прижатым к стенке".

В июне 2017 года газета The Washington Post писала, что Барак Обама, будучи президентом США, в 2016 году одобрил разработку электронных мер против России. Журналисты выяснили, что Обама принял такое решение в августе 2016 года, когда спецслужбы опубликовали секретный доклад, в котором говорилось, что Путин "лично принимал участие в организации киберкампании, направленной на то, чтобы навредить или дискредитировать президентские выборы в США".» ***(Нуланд рассказала о планах нанести Москве ответный кибердар // Українська служба швидких новин (https://sumynews.online/nuland-rasskazala-o-planax-nanesti-moskve-otvetnyj-kiberudar/). 11.03.2018).***

***

«Міністерство внутрішньої безпеки і Федеральне бюро розслідувань США опублікували спільний звіт щодо російських кібератак.

У ньому відомства описують багаторівневу кампанію з кібератак, націлених на урядові установи США й організації в галузях енергетики (зокрема ядерної), а також в торгівлі, водопостачання, авіації і на «критично важливі об'єкти».

Для здійснення атак використовувалися шкідливе програмне забезпечення та фішинг. Як наслідок, проросійським кібер-а́кторам вдавалося встановити віддалений доступ до вражених пристроїв та мереж й збирати конфіденційні дані…

Відомства також оприлюднили попередження, в якому закликали інші компанії в енергетичному секторі перевірити свої системи кіберзахисту…» ***(Американські спецслужби оприлюднили звіт з доказами кібератак Росії на урядові установи США // Електронна книга скарг України (http://www.reaction.org.ua/tech/amerikanski-specsluzhbi-oprilyudnili-zvit-z-dokazami-kiberatak-rosi%d1%97-na-uryadovi-ustanovi-ssha/). 20.03.2018).***

***

«…Сенатський комітет із розвідки напередодні виборів до Конгресу оприлюднив перший проект рекомендацій для запобігання зарубіжним кібератакам на виборчу систему США. Згідно з текстом документу, сенатори закликають Конгрес збільшити фінансування, щоб посилити захист системи.

Співробітники американських спецслужб неодноразово попереджали про можливі спроби Росії або інших країн втрутитися в проміжні вибори у листопаді, коли на кону стоятиме контроль за обома палатами Конгресу США, а в багатьох штатах пройдуть губернаторські та муніципальні вибори…

Федеральні чиновники повідомили, що в 21 із 50 штатів зіштовхнулися зі спробами злому виборчої системи російськими хакерами у 2016 році, при цьому, кілька атак були успішними…

Республіканці та демократи одностайно вирішили, що наразі в Міністерства внутрішньої безпеки занадто мало співробітників і засобів для того, аби боротися із вищезгаданою проблемою. Вони порекомендували Конгресу негайно ухвалити закон про виділення штатам додаткових коштів для боротьби з кібератаками на виборчу систему.

Сенатори також порадили Вашингтону «чітко дати зрозуміти» противникам, що атаки на вибори — ворожий акт, і відповідним чином реагувати на подібні дії…» ***(Кібератаки РФ: американські сенатори рекомендують посилити захист виборчої системи США // «Ракурс» (http://racurs.ua/ua/n102523-senatory-ssha-zaklykaut-posylyty-borotbu-zi-vtruchannyam-rosiyi-u-vybory). 21.03.2018).***

***

«Команда спецпрокурора США Роберта Мюллера установила, что хакером под ником Guccifer 2.0, с которым контактировал Роджер Стон – экс-советник Дональда Трампа по избирательной кампании, оказался офицером Главного управления Генштаба ВС РФ, более известное как Главное разведывательное управление (ГРУ)…

В частности, Guccifer 2.0, известный как "одинокий хакер", передал ресурсу WikiLeaks украденные электронные письма Национального комитета Демократической партии США.

Напомним, Роберт Мюллер расследует дело о вмешательстве России в американские президентские выборы 2016 года…

В январе 2017 года ЦРУ, АНБ и ФБР "с высокой уверенностью" заявили, что ГРУ РФ использовало Guccifer 2.0 для взлома серверов Демократической партии.

…однажды Guccifer 2.0 забыл активировать VPN и использовал свой настоящий IP-адрес. Это позволило установить американским следователям, что хакер на самом деле работал из штаб-квартиры ГРУ в Москве по улице Гризодубовой. Однако конкретное имя и звание источники издания раскрывать не стали…» ***(СМИ узнали о контактах человека Трампа с хакером, который оказался офицером спецслужб Путина // Апостроф (https://apostrophe.ua/news/world/2018-03-24/smi-uznali-o-kontaktah-cheloveka-trampa-s-hakerom-kotoryiy-okazalsya-ofitserom-spetsslujb-putina-/125150). 24.03.2018).***

***

«…Соединенные Штаты после подписи президента выделят четверть миллиарда долларов на противодействие России…

В среду вечером республиканцы и демократы провели дебаты и согласовали проект федерального бюджета на окончание текущего фискального года — до 30 сентября. Ожидаемо, впрочем, что в нем сохранились тенденции на укрепление "обороны" в связи с агрессией России… Общая сумма, выделенная для американских ведомств, составляет $1,3 трлн. Из них $700 млрд оборонных средств, которые были увеличены на $80 млрд.

В проекте бюджета заложены $250 млн конкретно на противодействие российскому вмешательству и агрессии — на два года работы Фонда

противодействия российскому влиянию. Противодействие будет осуществляться по нескольким статьям, открывающим сразу несколько фронтов: помощь Европе, Евразии и Центральной Азии, международное военное обучение и подготовка, иностранная военная помощь, а также борьба с оборотом наркотиков….

Есть в проекте раздел, 7070, непосредственно касающийся Украины и Грузии. Поскольку, как жертвы агрессии, обе страны находятся на передовой борьбы с российской экспансией. В общей сложности конгрессмены хотят выделить Грузии $105 млн, а Украине — $420 млн и еще $200 млн военной помощи. И в украинском "пакете" $30 млн отводятся на укрепление энергонезависимости от России, что актуализировано недавним стокгольмским поединком "Нафтогаза" и "Газпрома"…

Проект бюджета также предполагает принуждение Путина и Ко к миру через внутреннее влияние на российские процессы. Например, будут выделены средства на поддержку демократических программ в РФ, включая обеспечение свободы слова в интернете, защиту демократии и верховенства права…

В США учли печальный опыт 2016 г. и готовятся к дальнейшему вмешательству россиян в выборы. В законопроекте заложены $307 млн для ФБР на борьбу с кибератаками из России. Еще $380 млн в виде грантов для укрепления избирательной системы США на местах. Штаты проводят даже не апгрейд своей сети в госучреждениях, а нацелились на новую систему. Но сперва спецслужбам, в том числе ФБР, хотят поручить проверить каждый винтик и плату, особенно если в создании системы и ее комплектующих участвовали несколько стран. В Конгрессе намерены предупредить любую возможность для кибершпионажа и саботажа. И, согласно документу, прямо указываются потенциальные источники угрозы — Китай, Иран, КНДР и Россия…

Таким образом, Вашингтон подтвердил свою приверженность поддержке суверенитета, территориальной целостности Украины и Грузии, а также консолидации усилий по обе стороны Атлантики для ответа на действия России…» ***(Владислав ГИРМАН. Взять Путина в тиски. Что конгрессмены прописали в бюджете // DsNews (http://www.dsnews.ua/world/vzyat-putina-v-tiski-chto-kongressmeny-propisali-v-byudzhete-22032018220000). 22 .03.2108).***

***

«Президент США Дональд Трамп продовжив дію санкцій проти РФ через підривну діяльність Кремля проти Вашингтона у кіберсфері.

Текст указу опублікований на офіційній сторінці Білого дому…

«…надзвичайна ситуація в країні, оголошена 1 квітня 2015 року, повинна продовжувати свою дію після 1 квітня 2018 року», – йдеться в указі.

Таким чином, Трамп продовжив на наступний річний термін дію розпорядження президента Обами, яке запроваджувало санкції проти осіб, причетних до кіберактивності, що загрожувала нацбезпеці США…» ***(Трамп продовжив санкції проти Росії за підривну діяльність проти Вашингтона // Західна інформаційна корпорація (https://zik.ua/news/2018/03/28/tramp_prodovzhyv_sanktsii_proty_rosii_za_pidryvnu_diyalnist_proty_1294089). 20.03.2018).***

***

«Российское посольство в Лондоне выразило обеспокоенность отсутствием объяснения со стороны британского МИД по поводу звучавших со стороны некоторых парламентариев угроз задействовать «наступательный киберпотенциал» против России…

13 марта британские СМИ сообщили, что правительство Великобритании может рассмотреть возможность проведения секретной кибератаки против России в качестве «ответной меры» на отравление экс-полковника ГРУ Сергея Скрипаля. В российском посольстве отметили, что подобные угрозы были озвучены и в парламенте Великобритании.

В ответ российское посольство официально запросило разъяснения у МИД Великобритании об угрозе осуществления Лондоном кибератаки против России» ***(Алина Назарова. Лондон не стал объяснять угрозы кибератак против России // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/3/30/915238.html). 30.03.2018).***

***

«Различные государственные кибернетические системы Канады ежедневно испытывают более миллиарда кибератак.

Об этом заявила глава Центра безопасности коммуникаций Канады (спецслужбы, ответственной за радиоэлектронную борьбу - ред.) Грета Босенмайер…

"В среднем мы ежедневно блокируем более миллиарда вредных попыток вмешательства в правительственные системы", - сказала Босенмайер.

По её словам, в это число входят разнообразные операции: от незначительных атак, направленных на оценку прочности системы, до распространения вредоносных программ и целенаправленного взлома.

Она подчеркнула необходимость принятия в Канаде нового законодательства, которое бы позволило спецслужбе осуществлять наступательные операции…

По ее убеждению, такой подход позволил бы существенно повысить эффективность работы разведки…

Добавим, что в федеральный парламент уже был внесен правительственный законопроект, который предлагает расширить полномочия Центра по безопасности коммуникаций, в том числе позволив ему проведение наступательных операций…» ***(Более миллиарда кибератак ежедневно осуществляется на правительство Канады, - разведка // DsNews (http://www.dsnews.ua/world/bolee-milliarda-kiberatak-ezhednevno-osushchestvlyaetsya-na-29032018083900). 29.03.2018).***

***

«ФСБ подготовила законопроект, утверждающий порядок информирования о кибератаках на критическую информационную инфраструктуру (КИИ) России, реагирования на них и принятия мер по ликвидации их последствий…

Согласно проекту приказа, субъекты критической информационной инфраструктуры сообщают в ФСБ обо всех хакерских атаках, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании объектов КИИ, …направляя данные в Национальный координационный центр по компьютерным инцидентам (НКЦКИ)…

Субъект КИИ реагирует на хакерскую атаку и принимает меры по ликвидации ее последствий силами своих подразделений и должностных лиц…

Согласно законопроекту, субъекты КИИ разрабатывают план реагирования на кибератаки и принятия мер по ликвидации их последствий…

Не реже одного раза в год субъект КИИ организует и проводит тренировки по отработке мероприятий плана.

Субъект КИИ сообщает о результатах реагирования и ликвидации последствий кибератак в НКЦКИ в срок не позднее 48 часов после завершения таких мероприятий…» ***(Алина Пятигорская. ФСБ разработала порядок реагирования на кибератаки в отношении критической информационной инфраструктуры // «Парламентская газета» (https://www.pnp.ru/economics/fsb-razrabotala-poryadok-reagirovaniya-na-kiberataki-v-otnoshenii-kriticheskoy-informacionnoy-infrastruktury.html). 12.03.2018).***

***

«Керівники британських спецслужб попередили ключові енергетичні компанії про необхідність підвищити безпеку на тлі побоювань російської кібератаки…

Представники Національного центру кібербезпеки (NCSC) надали поради компанії The National Grid, яка займається поставками електрики і газу в Англії та Вельсі, як покращити свій захист, щоб запобігти відключенню енергії.

Компанії із постачання електроенергетики, газу та води, атомна електростанції Селлафілд, департаменти Уайтхолла та лікарні були попереджені про ймовірну підготовку підтримуваної Кремлем хакерської атаки після отруєння у Солсбері.

Чиновники NCSC повідомили ключовим організаціям, що вони можуть зіткнутися зі спробами викрадення даних платників податків та пацієнтів або атаками, що можуть зупинити роботу їхніх сайтів…» ***(Спецслужби Британії попередили енергокомпанії про кібератаки через Солсбері // Європейська правда (http://www.eurointegration.com.ua/news/2018/03/18/7078937/). 18.03.2018).***

***

«…По его словам заместителя генерального директора компании Positive Technologies Бориса Симиса, в 2017 году проявилась весьма опасная

тенденция, показавшая, что даже хорошо защищенные критические инфраструктуры могут быть взломаны путем простых кибератак. В качестве примера специалист привел масштабную эпидемию WannaCry, от которой пострадали организации во всем мире…

Он выделил еще одну важную прошлогоднюю тенденцию – всплеск целенаправленных атак, в рамках которых злоумышленники собирают доступную информацию о жертве, в том числе используемые антивирусы и межсетевые экраны, а затем с помощью методов социальной инженерии узнают должности и адреса сотрудников целевой организации, а затем атакуют их, используя персонифицированные вредоносные фишинговые письма, отправленные якобы от имени, например, контролирующих органов…

Третий вектор атак, получивший распространение в последнее время, направлен преимущественно на банки. Поскольку сами банки хорошо защищены с точки зрения информационной безопасности и атаковать их сложно и дорого, преступники выбирают более простой путь и атакуют компании-поставщики финорганизаций. Взломав системы поставщика, хакеры от имени его настоящего сотрудника отправляют в банк инфицированное письмо, получая таким образом доступ к банковской сети.

Как считает Симис, с появлением новых угроз изменилась парадигма защиты объектов КИИ, и концепцию Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) можно рассматривать как проявление наблюдаемых перемен. …В стратегии защиты появилось два новых направления: с одной стороны организации стараются усложнить киберпреступникам взлом, а с другой ставится задача научиться оперативно выявлять скрытые инциденты – не через год или два, а хотя бы в течение месяцев или недель.

По словам специалиста, идея создания центров ГосСОПКА не требует появления каких-то новых новых продуктов и услуг. Для создания ведомственных центров и организации их взаимодействия с главным центром ГосСОПКА достаточно того набора решений, который используется в обычных центрах мониторинга информационной безопасности (Security Operation Center, SOC) коммерческих компаний…» ***(Эксперт Positive Technologies рассказал о новых векторах атак на объекты КИИ и стратегическом значении системы ГосСОПКА // SecurityLabRu (https://www.securitylab.ru/news/492214.php). 20.03.2018).***

***

«Авиация, как часть транспортного сектора, входит в критическую инфраструктуру. В последнее время эксперты все чаще говорят о киберрисках, которым она подвергается благодаря новым технологиям — например, подключенные к Сети развлекательные системы на борту. Для противостояния этим киберрискам финляндская компания F-Secure запускает новые службы авиационной кибербезопасности Aviation Cyber Security Services, которые помогут защитить не только самолеты, но и всю отрасль…

Новая услуга будет объединять в себе оценки безопасности наземных систем и линий передачи данных, сканеров уязвимостей, мониторинга безопасности, служб реагирования на инциденты и специальной подготовки кибербезопасности для персонала. «Ключевой мерой защиты является разделение систем на разные доверительные домены, а затем осуществление контроля за тем, как системы в разных доменах могут взаимодействовать друг с другом. Это поможет ограничить воздействие, например, доступного для пассажиров Wi-Fi на критически важные для безопасности системы, такие как управление воздушным судном», — объясняет F-Secure.» ***(Олег Иванов. F-Secure поможет снизить киберриски авиационной промышленности // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-03-20-1447/25761). 20.03.2018).***

***

«…киберугрозы вытеснили чрезмерное регулирование с первого места в списке рисков для банковского сектора и рынков капитала. Такие выводы сделала компания PwC после очередного ежегодного опроса руководителей крупнейших компаний мира.

89% участников опроса обеспокоены кибербезопасностью, тогда как 93% запланировали на 2018 год значительные инвестиции в обеспечение кибербезопасности.

За прошедший год увеличилось количество руководителей сегмента, считающих темпы технологического прогресса (85%) и тесно связанные с ними изменения в поведении клиентов (73%) угрозой для своего бизнеса…

Примечательно, что поиск квалифицированных сотрудников с цифровой компетенцией широко признается трудноосуществимой задачей: менее 20% CEO считают эту задачу легкой. Тогда как в основном под такими специалистами подразумеваются разработчики приложений, инженеры-робототехники и аналогичные специалисты, не менее важно наличие знаний о новых технологиях и у других сотрудников организации, включая ее высшее руководство…» ***(Риск киберугроз в банковском секторе стал намного выше — исследование // PaySpaceMagazine (https://psm7.com/news/risk-kiberugroz-v-bankovskom-sektore-stal-namnogo-vyshe-issledovanie.html). 28.03.2018).***

***

«Больницы и медицинские устройства постоянно находятся под атакой. В прошлом году вымогатели Wannacry заразил два устройства медицинской компании Bayer и оставил сотни больниц с парализованными компьютерными системами…

Можно было бы ожидать, что больницы будут иметь надежные стратегии по кибер-безопасности, однако множество компаний по-прежнему использует устаревшие решения. Отсутствие бюджета, ресурсов и сложные инфраструктуры, что делает сети больниц хорошими целями, которые стоит немедленно защитить…

Больницы оказываются прибыльной целью для кибер-преступников. Вымогатели имеет возможность хранения необходимого медицинского оборудования в качестве заложника. Без подключения к мониторам сердечного

ритма или других устройств, больницы не имеют другого выхода, как платить выкуп в случае нападения…

Внедрение следующих рекомендаций поможет больницам защитить сеть, документацию пациентов и медицинское оборудование перед хакерами и вредоносных кибератак:

Резервное копирование важных файлов. Необходимо создавать резервную копию медицинской документации и истории болезни пациента в автономном режиме на внешнее устройство…

Необходимо обратить внимание сотрудников, что не следует открывать электронные письма, которых не ожидали, что не должны нажимать на ссылки, если они получены из известного и ненадежного источника, а документ попросят запуск макросов в файле Office тем более не должны этого делать!

Внедрение решений безопасности высокого качества, обеспечивающие защиту сети от различных видов вредоносных программ и угроз, связанных с программным обеспечением. Сегодняшние решения могут обнаруживать и блокировать офисные документы, содержащие вредоносные макросы и предотвратить его попадание в систему (так называемый exploit kits).

Вымогательство становятся все более популярным способом получения крупных денежных сумм злоумышленниками, так как платежи обычно осуществляются анонимно — например, с помощью кошельков Bitcoin. Киберпреступники используют слабости больниц, угрожая здоровью пациентов…» ***(Карина Юнкова. Больницы на мушке хакеров // Bad Android (https://bad-android.com/blogs/31797-bolnitsy-na-mushke-khakerov). 29.03.2018).***

***

Кіберзлочинність та кібертероризм

«Одиннадцать человек, включая охранника, были арестованы в Исландии в связи с кражей из местных дата-центров оборудования для майнинга криптовалют на сумму 2 млн долларов…

На самом деле было совершено четыре кражи: три в декабре и одна в январе. Полиция некоторое время не рассказывала об этом общественности, чтобы не скомпрометировать расследование.

Две из краж были совершены на юго-западном полуострове Рейкьянес…

Исландия - популярное место для майнинга криптовалют, поскольку этот процесс чрезвычайно энергоемкий, а энергия из возобновляемых источников в Исландии дешевая. …сейчас исландская полиция контролирует использование энергии на всей островной территории, чтобы найти украденное оборудование…» ***(Ирина Фоменко. Воровство криптовалюты в Исландии повлекло за собой 11 арестов // Internetua (http://internetua.com/vorovstvo-kriptovaluat-v-islandii-povleklo-za-soboi-11-arestov). 06.03.2018).***

***

«В среду произошла мощнейшая в истории интернета DDos-атака, пострадал крупный веб-сервис для хостинга IT-проектов GitHub.

Кибератака произошла в среду около 22.15 (UTC-4)… Мощность атаки составила 1,35 терабита в секунду…

В течение 10 минут платформа запрашивала автоматическую помощь от службы борьбы с DDos-атаками Akamai Prolexic. Сервис маршрутизировал входящий и исходящий трафик от GitHub, проведя данные через собственные центры защиты, чтобы отсеять вредоносные пакеты данных.

Спустя восемь минут кибератака сошла на нет. По словам вице-президента по безопасности компании Akamai Prolexic Джоша Шаула, атака на GitHub стала самой мощной за всю историю интернета…» ***(Алексей Ласнов. Произошла самая мощная DDos-атака в истории интернета // «Парламентская газета» (https://vz.ru/news/2018/3/2/910779.html). 02.03.2018).***

***

«Кибератакам в 2017 году подверглись 72% медицинских учреждений во всем мире, были зафиксированы попытки заразить вирусами почти треть устройств в этих организациях. Такие данные привел руководитель российского исследовательского центра “Лаборатории Касперского” Юрий Наместников в ходе конференции по кибербезопасности Security Analyst Summit (SAS 2018).

Исследование было проведено в 2017 году на основании данных 1,5 тыс. организаций и 70 тыс. используемых ими устройств.

По словам Наместникова, 57% медицинских организаций подверглись кибератакам через интернет (или также через электронную почту), а в систему 62% организаций вирусы попадали через физические носители. Чаще всего хакеры пытались атаковать медучреждения на Филиппинах, в Венесуэле, Таиланде, Парагвае и ОАЭ.

Злоумышленники также интересовались фармацевтическими компаниями – в 2017 году 78% организаций из этой сферы подверглись атакам, попытки заражения затронули порядка 45% устройств. Две трети фармкомпаний было атаковано через интернет, 72% – через физические носители. Наиболее часто злоумышленники атакуют фармкомпании Бангладеш, Индонезии и Марокко, а также на Шри-Ланке и в Индии…» ***(В 2017 году 57% медицинских организаций подверглись кибератакам через интернет // mResearcher (https://mresearcher.com/2018/03/v-2017-godu-57-meditsinskih-organizatsij-podverglis-kiberatakam-cherez-internet.html). 10.03.2018).***

***

«…Согласно результатам мониторинга Positive Technologies, злоумышленники следят за абонентами, перехватывают звонки, обходят системы тарификации, блокируют пользователей. Только один крупный оператор с абонентской базой в несколько десятков миллионов человек ежесуточно подвергается более чем 4 тысячам кибератак.

Проекты по мониторингу безопасности в сетях SS7 проводились для крупных операторов связи Европы и стран Ближнего Востока. Атаки с целью

мошенничества, нарушения доступности абонентов, перехвата абонентского трафика (в том числе звонков и SMS-сообщений) в сумме составили менее двух процентов. Однако подобные угрозы являются наиболее опасными для пользователей.

Согласно результатам исследования, успешными для злоумышленников являются 100% атак, направленных на перехват SMS-сообщений. При этом кража передаваемых таким образом одноразовых кодов чревата компрометацией систем ДБО, мобильных банков, интернет-магазинов, порталов государственных услуг и множества других сервисов…

Другой вид атак — отказ в обслуживании — представляет угрозу для электронных устройств интернета вещей. Сегодня к сетям мобильной связи подключены не только отдельные устройства пользователей, но и элементы инфраструктуры умных городов, современные промышленные предприятия, транспортные, энергетические и иные компании.

Серьезные опасения связаны и с мошенничеством в отношении оператора или абонентов. Существенная часть таких атак пришлась на несанкционированную отправку USSD-запросов (81%). Подобные запросы позволяют осуществить перевод денег со счета абонента, подписать абонента на дорогостоящую услугу или отправить фишинговое сообщение от имени доверенного сервиса.

Безопасность сетей мобильной связи все еще находится на низком уровне, что подтверждается результатами работ по анализу защищенности сетей SS7, представленными в первой части отчета. В выборку попали данные 24 наиболее информативных проектов в сетях операторов стран Европы (в том числе России) и Ближнего Востока в 2016—2017 годах, половина которых имеют объем абонентской базы более 40 миллионов человек.

Практически в каждой сети можно прослушать разговор абонента или прочитать входящие SMS-сообщения, а мошеннические операции можно успешно проводить в 78% сетей. Все сети содержат опасные уязвимости, которые позволяют нарушить доступность сервисов для абонентов…

В отчете отмечается, что только комплексный подход к решению проблем безопасности, включающий регулярное проведение анализа защищенности, поддержание настроек сети в актуальном состоянии, постоянный мониторинг сигнального трафика и своевременное выявление нелегитимной активности, может обеспечить высокий уровень защиты от преступников» ***(100% реальных атак по перехвату SMS-сообщений достигают цели // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5478766-100-realnyx-atak-po-perexvatu-SMSso.html#ixzz5ABudgKQb). 05.03.2018).***

***

«Злоумышленники чаще атакуют веб-приложения банков и электронных торговых площадок, потому что успешные взломы приносят ощутимую финансовую выгоду…

Такие данные опубликовали эксперты Positive Technologies по итогам статистики, полученной в результате пилотных проектов по внедрению межсетевого экрана PT Application Firewall в организациях различных отраслей.

Четвертый квартал подтвердил основные тренды прошлых обзоров. Самыми популярными атаками вновь стали «Межсайтовое выполнение сценариев» и «Внедрение SQL-кода» — суммарно они составляют практически половину от всех атак.

Как и в прошлые периоды, аналитики отметили незначительное увеличение интенсивности атак в дневные и вечерние часы; большая часть атак направлена на пользователей веб-ресурсов, которые в это время особенно активны.

Однако инциденты безопасности возникают также и в ночные и утренние часы: часто злоумышленники проводят атаки в это время с расчетом на то, что службы безопасности компаний не смогут своевременно обнаружить атаку и отреагировать должным образом…

Практически половина атак на веб-ресурсы производилась с российских IP-адресов. В топ-5 источников атак, помимо России, входят США, Китай, Франция и Германия.

В среднем число атак в сутки в IV квартале варьировалось от 200 до 300 и крайне редко опускалось ниже 100…

Максимальное число зафиксированных атак в день на одну компанию по всем пилотным проектам составило 34 629» ***(Веб-приложения банков и торговых площадок стали главной целью хакеров // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5480861-Vebprilozheniya-bankov-i-torgovyx.html#ixzz5AC38468i). 15.03.2018).***

***

«Американские чиновники, их союзники и эксперты в области безопасности опасаются новых мощных кибератак на промышленные заводы по всему миру, подобных той, что была осуществлена на некую нефтехимическую компанию в Саудовской Аравии в августе минувшего года…

Специалисты, ведущие расследование инцидента, не раскрывают подробности об атаке, а также не называют компанию, которая стала ее жертвой. Пока им не удалось идентифицировать злоумышленников, стоящих за нападением. …Техническими возможностями для проведения подобных атак обладают ряд стран, в том числе Иран, Китай, Россия, США и Израиль, говорят эксперты.

…Известно, что в ходе атаки злоумышленники скомпрометировали защитные контроллеры Triconex производства компании Schneider Electric. Данные решения используются на порядка 18 тыс. промышленных объектов по всему миру, включая атомные электростанции, очистные сооружения, нефтегазоперерабатывающие объекты и химзаводы…

В ходе расследования специалисты обнаружили на одном из компьютеров странный файл, который выглядел как часть контроллера Schneider, но предназначался для саботажа системы. Следователям не удалось определить, как этот файл оказался на компьютере, но они исключают инсайдерскую работу. Взрыва не произошло лишь по той причине, что в коде злоумышленников содержалась ошибка, однако работа завода все же была нарушена. К настоящему времени преступники уже наверняка устранили ошибку и всего лишь дело времени, когда они проведут похожую атаку на другие промышленные системы,

считают эксперты» ***(Эксперты опасаются новых смертельных кибератак на нефтезаводы по всему миру // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=121995). 16.03.2018).***

***

«Китайские разведывательные агентства изменяют в Китайской национальной базе данных об уязвимостях (CNNVD) информацию о проблемах безопасности для содействия хакерам, связанным с правительством КНР. Об этом сообщили эксперты из аналитической компании Recorded Future в своем отчете.

Согласно докладу, за последние несколько месяцев были зафиксированы массовые внесения изменений в базу данных web-сайта CNNVD. В частности, операторы базы данных внесли информацию о нескольких сотнях уязвимостей задним числом.

По словам аналитиков, подобные случаи начались в ноябре минувшего года после публикации отчета, в котором Recorded Future обвинила CNNVD в задержке раскрытия критических уязвимостей для того, чтобы дать киберподразделениям китайской разведки больше времени на оценку потенциальной пользы от эксплуатации данных проблем.

Как сообщили специалисты, за последний год в CNNVD была отредактирована информация о дате публикации по меньшей мере 267 критических уязвимостей…

Как полагают аналитики, задержка раскрытия критических уязвимостей, скорее всего, осуществляется для сокрытия данных о проблемах безопасности от местных компаний, которые полагаются на CNNVD. Таким образом спецслужбы могут тщательно следить за китайскими внутренними организациями» ***(Китайские спецслужбы задерживают публикацию данных об уязвимостях // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=121879). 12.03.2018).***

***

«Эксперты Avast обнародовали новые сведения о прошлогоднем инциденте с CCleaner.

…согласно докладу, представленному на конференции SAS в Мексике, хакеры, проведшие атаку на инфраструктуру CCleaner и добавившие бэкдор в данную утилиту, также готовились к заражению уже скомпрометированных компьютеров новой разновидностью вредоносного программного обеспечения.

Инцидент произошел в сентябре прошлого года, когда специалисты Avast выявили вредоносную программу, внедренную в 32-разрядные версии CCleaner v5.33.6162 и CCleaner Cloud v1.07.3191. Как утверждают эксперты, вредоносная программа заразила около 22700000 компьютеров, похищая при этом лишь такие базовые сведения, как имя компьютера и данные о домене.

Позже выяснилось, что внедрение данной программы являлось всего лишь начальным этапом крупномасштабной киберкампании для поиска компьютеров, подключенных к внутренним сетям таких корпораций, как Akamai, Cisco, Google, Intel, Microsoft и Oracle. В рамках второго этапа хакеры внедрили вредоносную

программу в 40 компьютеров. Как утверждают эксперты Avast, Cisco Talos и «Лаборатории Касперского», атаку организовала кибергруппировка Axiom, которая, вероятно, «работает» с территории Китая.

Согласно докладу, представленному на конференции в Мексике, хакеры также готовились к третьему этапу киберкампании. На компьютерах сотрудников компании-разработчика CCleaner – Piriform – удалось обнаружить образец вредоносной программы, которая присутствовала там с 12 апреля прошлого года. По мнению экспертов, злоумышленники применяли сети Piriform для подготовки основного взлома.

Обнаруженная программа называется ShadowPad…

Специалисты Avast утверждают, что программа ShadowPad должна была применяться на третьем этапе киберкампании. Однако ИБ-экспертам заблаговременно удалось обнаружить инфицированную версию CCleaner, помешав планам злоумышленников» ***(Хакеры, которые взломали CCleaner, хотели провести новую вредоносную кампанию // SecureNews (https://securenews.ru/ccleaner_2/). 13.03.2018).***

***

«Департамент юстиції США звинуватив іранський уряд у фінансуванні масової хакерської схеми, націленої на викрадення наукових дослідженнь…

У п’ятницю Департамент юстиції звинуватив дев’ять іранців у зв’язку з кібермахінаціями. Звинувачувальний вирок свідчить про те, що хакерство було здійснено від імені Корпусу вартових Ісламської революції — одного з провідних підрозділів розвідки іранського уряду…

Дев’ять обвинувачуваних, всі — громадяни і мешканці Ірану, були пов’язані з Іранським інститутом Мабна, заявили в Департаменті юстиції. Повідомляється, що вони змогли вкрасти більше 31 терабайтів академічних даних та інтелектуальної власності, відповідно до судових документів.

Загалом, понад 144 американських університетів, 176 університетів 21 зарубіжних країн, 47 американських та іноземних компаній приватного сектору, Міністерство праці США, Федеральна комісія з регулювання енергетики, Штати Гаваї та Індіана, Організація Об’єднаних Націй та Дитячий фонд Організації Об’єднаних Націй стали жертвами “кіберкрадіжки”…» ***(Саша Картер. У США звинуватили уряд Ірану у масштабній "кіберкрадіжці" // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1721735-u-ssha-zvinuvatili-uryad-iranu-u-masshtabniy-kiberkradizhtsi). 23.03.2018).***

***

«…Специалисты Positive Technologies собрали статистику эффективности атак с применением методов социальной инженерии. В ходе проектов по анализу защищенности корпоративной инфраструктуры эксперты компании имитировали активность хакеров и отправляли сотрудникам компаний-заказчиков сообщения, содержащие вложенные файлы, ссылки на веб-ресурсы и формы для ввода паролей. Всего было отправлено 3332 письма…

Самым эффективным методом социальной инженерии оказались сообщения с фишинговой ссылкой: по ней перешли 27% получателей. Пользователи невнимательно читают адрес или даже просто, не глядя, кликают на него и переходят на поддельный сайт…

Сотрудники часто не просто открывают незнакомые файлы и кликают по подозрительным ссылкам, но и вступают в переписку со злоумышленниками. В 88% случаев это делают работники, не связанные с IT (бухгалтеры, юристы, менеджеры и т. п.). Каждый четвертый участник такой переписки оказался руководителем отдела. Впрочем, на удочку хакеров могут попадаться даже специалисты по безопасности: в ходе наших экспериментов 3% из них вступили в диалог.

В ходе беседы с хакером пользователи могут жаловаться на то, что присланные зловредные файлы или ссылки не открываются, — в некоторых случаях перед этим они пробовали открыть файлы или ввести пароль по ссылке по 30–40 раз! Часто, если открыть файл сразу не удается, сотрудник пересылает письмо в IT-департамент компании с просьбой о помощи. Это увеличивает риски компрометации инфраструктуры, поскольку технические специалисты доверяют коллегам и с высокой вероятностью запустят файл…

Эффективность рассылок от лица поддельных компаний сегодня снижается (11% потенциально опасных действий), в то время как если сообщение приходит от имени реальной компании и реального человека, вероятность успеха взломщиков возрастает (33%)…

Киберпреступники используют страх, жадность, надежду и другие эмоции для повышения эффективности своих атак. Поэтому в темах своих писем они используют фразы вроде «список сотрудников на увольнение» (спровоцировали 38% потенциально опасных действий), «выплаты премий за год» (25%) и т. п. При получении таких сообщений люди часто забывают об элементарных правилах безопасности…

«Наше исследование процессов обеспечения ИБ в российских компаниях показало, что 38% организаций вообще не проводят тренинги для сотрудников по вопросам ИБ, а 37% делают это формально, без какой-либо проверки эффективности, — комментирует аналитик Positive Technologies Дмитрий Каталков…» ***(Отчет Positive Technologies: социальная инженерия открывает хакерам двери вашей компании // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/291395/). 23.03.2018).***

***

«…Анализ криминогенной обстановки, проведенный МВД Беларуси, свидетельствует о перманентном росте количества преступлений в сфере высоких технологий: в 2017 году этот показатель увеличился на 25% (с 2471 в 2016 году до 3099 в 2017 году). При этом основной объем киберпреступлений в стране – около 75% – приходится на хищения денежных средств, сопряженные с несанкционированным доступом к компьютерной информации (квалифицируется по ст. 212 УК Беларуси). Количество выявленных преступлений в сфере информационной безопасности, предусмотренных статьями 349-355 УК, также

увеличилось на 20% (с 651 до 781 уголовного дела). Среди них: объем инцидентов по неправомерному завладению компьютерной информацией (вырос на 52%), модификация компьютерной информации (на 48%) и несанкционированный доступ к компьютерной информации (на 45%)…

В связи с ухудшением ситуации с кибербезопасностью в Беларуси компания Group-IB сообщила о планах открытия представительства в Беларуси. Главой Group-IB в регионе назначен Александр Сушко, занявший позицию руководителя по развитию бизнеса…

По словам Александра Сушко и к белорусским гражданам, и к белорусским предприятиям, включая банковские учреждения, пришло осознание реальности киберугроз и необходимости проведения мероприятий, направленных на защиту данных пользователей в Интернет, только в последние 3-4 года…

Кроме того, в Group-IB прогнозируют, что, пользуясь инструментарием, ранее «обкатанным» на банковской инфраструктуре, хакерские группы будут переключать свое внимание с белорусских банков на криптоиндустрию. В фокусе – атаки на ICO крипто-проектов, кошельки криптовалют, аккаунты криптобирж… По словам Сушко, в Беларуси в настоящее время регистрируются единичные факты хищений криптовалютных средств. Однако рост таких преступлений – вопрос времени: уже в конце марта законодательство в этой сфере изменится, что увеличит количество участников крипторынка и неизбежно привлечет хакеров.

Помимо регулярного мониторинга белорусского рынка информационной безопасности, перед своим представительством в регионе штаб-квартира Group-IB ставит задачу поиска перспективных направлений для развития, в том числе, за счет инвестиций, а также создание канала продаж продуктов и услуг компании, направленных на выявление и предотвращение кибератак в государственном и коммерческом секторе. На данный момент, среди наиболее перспективных ниш для регионального рынка в компании видят сегмент решений по обнаружению целевых атак, защите корпоративных порталов, раннее обнаружение и предупреждение кибератак, а также аналитические системы безопасности с использованием технологии BIG DATA...» ***(Белорусские компании могут стать новой крупной мишенью для хакеров // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5486841-Belorusskie-kompanii-mogut-stat-nov.html#ixzz5As9cJoi1). 26.03.2018).***

***

«Дослідники безпеки з компанії Armor опублікували звіт про підпільні ринки в даркнеті…

Згідно з доповіддю, DDoS-атаку можна замовити всього за $10 за годину, $200 за день або за $500 - $1 тис. за тиждень. Дослідники також виявили в продажу банківські ботнети (оренда коштує $750 на місяць), набори експлойтів ($1400 на місяць), експлоїти для вразливостей в WordPress ($100), скімери ($1500) і хакерські навчальні програми ($50).

Найбільш поширеним товаром в даркнета залишаються дані банківських карт. Ціна варіюється в залежності від країни походження.

Різна інформація про кредитні картки, часто отримана за допомогою шкідливих програм для PoS-терміналів або в інтернеті, коштує дешевше, проте повні дані, необхідні для створення копій карт, обійдуться в два або три рази дорожче.

Шахраї також можуть купити доступ до зламаним банківських рахунків. Ціни на рахунку варіюються в залежності від суми грошей, яка на них зберігається…

Ринки та форуми «Тіньової павутини» також пропонують безліч зламаних облікових записів. Доступ до зламаних акаунтів в соціальних мережах в середньому коштує близько $13. Хакери можуть пропонувати доступ до облікових записів в Facebook, Twitter, Instagram, Hulu, Netflix, Spotify, Amazon, Skype та ін…» ***(У даркнеті можна замовити DDOS-атаку за $10 за годину // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/03/22/10-dollars-for-DDOS.html). 22.03.2018).***

***

«Чтобы определить уровень опасности от кибератак на незащищенные базы данных MongoDB, ИБ-эксперты из Kromtech решили провести эксперимент, в рамках которого специально разместили открытую для подключений извне базу MongoDB и стали отслеживать входящие соединения.

Как утверждают эксперты, в базе хранилось 30 гигабайт фальшивой информации. За три часа хакеры обнаружили базу, оставили требование о выкупе в 0,2 биткоина, а через 13 секунд уничтожили все хранившиеся там данные.

…нынешняя атака на базу данных была проведена с территории Китая.

Эксперты выразили уверенность, что подобная задача могла быть завершена в течение 13 секунд лишь с помощью автоматизированного сценария…

Эксперты советуют пользователям обеспечить надлежащую защиту для своих баз данных, так как неправильно настроенные серверы MongoDB всегда находятся под угрозой атаки со стороны хакеров…» ***(Хакеры уничтожили базу данных MongoDB, потребовав выкуп за 13 секунд до этого // SecureNews (https://securenews.ru/mongodb_2/). 26.03.2018).***

***

«Международная компания Group-IB, занимающаяся кибербезопасностью, сообщила, что мошенники умудрились нажиться на сбое в работе мессенджера Telegram.

Через несколько часов после начала сбоя, около 11:00 мск, в ветке обсуждений в аккаунте Дурова в Твиттере дважды появилось сообщение якобы от лица владельца Telegram с приглашением поучаствовать в «извинительной кампании», которая представляла собой лотерею. Аватар и имя владельца у аккаунта, публиковавшего сообщения, были такими же, как у Павла Дурова, отличалось лишь название учётной записи — @durhiov вместо @durov…

Сообщение об «акции» собрало около тысячи лайков и 45 репостов. В результате за час мошенники успели получить 78,4568202 ETH ($31 876).

Специалисты из Group-IB обращают внимание на то, что сообщение о лотерее тиражировали боты и оно сопровождалось комментариями «счастливых

победителей», что указывает на хорошую подготовку и планирование со стороны злоумышленников.

Вскоре внимательные пользователи начали предупреждать остальных об обмане, однако фальшивый аккаунт до сих пор не заблокирован.

Причиной многочасового сбоя в работе Telegram, затронувшего пользователей в Восточной Европе, в Африке и на Ближнем Востоке, стало отключение питания европейских серверов компании» ***(Мошенники заработали больше $30 000 в криптовалюте на сбое Telegram // BIGFIN (https://bigfin.net/29/03/2018/moshenniki-zarabotali-bolshe-30-000-v-kriptovaljute-na-sboe-telegram/). 29.03.2018).***

***

Діяльність хакерів та хакерські угруповування

«После рассказа Владимира Путина о «фантастическом оружии, готовом поражать любые цели», неизвестные хакеры поразили российский АО «Государственный ракетный центр имени Макеева»…

В воскресенье на сайте российского госпредприятия появился «черный властелин» – интернет-мем в образе некоего афроамериканца, одетого в гей-стиле, обозначающий, как правило, грозящее наказание. Мем сопроводили надписью «PUTIN MOYA RAKETA GOTOVA»…

Об обнаруженном "взломе" стало известно в воскресенье утром. Кто именно подшутил над путинскими ракетостроителями – неизвестно…» ***(Владимир Кондрашов. Российский ракетный центр опубликовал фото «черного властелина» // Internetua (http://internetua.com/rossiiskii-raketni-centr-opublikoval-foto-csernogo-vlastelina-). 05.03.2018).***

***

«Група хакерів, яка нещодавно атакувала урядові сайти Німеччини, викрала документи, що стосувалися України та Brexit. Про це з посиланням на власні джерела повідомляє Der Spiegel…

Також видання відзначає, що витік документів щодо України та Білорусі був контрольований. Тобто файли зникли тоді, коли служба безпеки уже була поінформована про кібернапад…» ***(Тоня Туманова. Документи щодо Brexit та України: стало відомо, що вкрали хакери у Німеччини // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1719346-dokumenti-schodo-brexit-ta-ukrayini-stalo-vidomo-scho-vkrali-khakeri-u-nimechchini). 10.03.2018).***

***

«…Кібератака російських хакерів на урядову мережу Німеччини, про яку стало відомо наприкінці лютого, завершилася невдачею. Хакери не змогли отримати доступ до захищеної інформації…

Хакери змогли проникнути в сервери німецького міністерства закордонних справ (МЗС) через мережеву інфраструктуру курсів підвищення кваліфікації для німецьких дипломатів. Їм вдалося це завдяки тому, що вони встановили на комп'ютері шкідливі програми.

Але інформація за межами цього з'єднання для них залишилася закритою. Хакери не змогли дістатися до документів МЗС та прав адміністратора…

Встановлено, що хакерська атака була здійснена наприкінці 2016 року, а виявлена в кінці 2017 року.

ЇЇ приписують хакерській групі APT28, відомій також під назвою Fancy Bear. Фахівці вважають, що вона працює під керівництвом Головного розвідуправління (ГРУ) збройних сил Росії...» ***(Російські хакери зазнали невдачі в кібератаці на урядову мережу Німеччини — DW // «Ракурс» (http://racurs.ua/ua/n102381-rosiyski-hakery-zaznaly-nevdachi-v-kiberataci-na-uryadovu-mereju-nimechchyny-dw). 18.03.2018).***

***

«Відому російську кібершпигунську групу Fancy Bear вважають причетною до низки атак на чорногорські інституції минулого року.

Про це повідомляє Balkaninsight з посиланням на Birn, Мережу балканських журналістських розслідувань.

На початку січня 2017 року на електронну пошту представника Міністерства оборони країни прийшов начебто звичайний лист від НАТО на тему: "NATO_secretary_meeting.doc".

Однак експерти стверджують, що повідомлення було відправлено не НАТО, а російською групою хакерів, які хотіли зламати урядову ІТ-систему та викрасти таємну інформацію.

Також в січні, за даними джерел Birn, уряд у Подгориці отримав ще два аналогічних повідомлення.

За даними трьох міжнародних ІТ-компаній з безпеки, всі ці листи прийшли від групи APT28, також відомої як Fancy Bear, яку спецслужби США пов'язують із Головним розвідувальним управлінням Генштабу РФ.

Чиновники Євросоюзу також вважають, що Чорногорія зазнала серйозної кібератаки в червні 2017 року…

Якщо у 2013 році було зафіксовано лише 22 таких інцидента, то за дев'ять місяців 2017 року їх було вже майже 400.

Багато з цих нападів, як вважають, пов'язані з рішенням країни вступити в НАТО, яке розлютило Росію…» ***(За низкою минулорічних кібератак на Чорногорію стоять хакери з РФ – розслідування // Європейська правда (http://www.eurointegration.com.ua/news/2018/03/5/7078382/). 05.03.2018).***

***

«В США утверждают, что российские хакеры в начале 2017 года провели кибератаку на систему гражданской авиации страны.

Исполнительный директор Центра обмена и анализа авиационной информации Джефф Трой заявил в пятницу, что кибератака имела «ограниченное воздействие»…

По мнению журналистов, слова Троя являются еще одним подтверждением кибератаки, описанной правительством США в четверг. Тогда сообщалось, что американские спецслужбы зафиксировали атаки якобы российских хакеров на критическую инфраструктуру страны.

В документе, опубликованном министерством внутренней безопасности США и ФБР, утверждается, что действия якобы правительства России были направлены против «органов власти США, а также организаций в энергетических, ядерных сферах, водных, авиационных и критически важных секторах производства и коммерческих объектов».

США неоднократно обвиняли Россию в хакерских атаках. В феврале консультанты Белого дома включили Россию в список государств-хакеров…» ***(Алексей Ласнов. Российских хакеров обвинили в проникновении в систему гражданской авиации США // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/3/16/912887.html). 16.03.2018).***

***

«За атаками на IT-инфраструктуру Олимпийских игр в Пхёнчхане стояла совсем не та кибергруппировка, на которую указывали все следы…

Напомним, что червь Olympic Destroyer смог на время парализовать олимпийские IT-системы незадолго до церемонии открытия Игр…

Спустя несколько дней после обнаружения Olympic Destroyer разные исследователи утверждали, что за ним стоят атакующие из России, Китая или Северной Кореи. Эксперты «Лаборатории Касперского» поначалу склонялись к последнему варианту, поскольку некоторые части кода этого червя на 100% совпадали с компонентами, использовавшимися известной кибергруппировкой Lazarus, имеющей северокорейское происхождение…

Однако при расследовании инцидентов непосредственно на месте в Южной Корее аналитики «Лаборатории Касперского» обнаружили ряд несоответствий между Olympic Destroyer и Lazarus… В итоге выяснилось, что те компоненты кода Olympic Destroyer, которые совпадали с кодом ПО Lazarus, на самом деле были искусно подделаны таким образом, чтобы максимально соответствовать особенностям северокорейской группировки…

Кто на самом деле стоит за киберинцидентами, случившимся во время последней зимней Олимпиады, достоверно пока неизвестно... Однако эксперты «Лаборатории Касперского» выяснили, что атакующие использовали обеспечивающий конфиденциальность сервис NordVPN и хостинг-провайдер MonoVM, которые принимают к оплате биткойны. Эти приёмы (наряду с некоторыми другими обнаруженными техниками) ранее встречались в операциях русскоговорящей группировки Sofacy» ***("Олимпийские" хакеры почти обманули экспертов по кибербезопасности // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5480119-Olimpijskie-xakery-pochti-obmanuli.html#ixzz5AC1Ats2e). 13.03.2018).***

***

«Кибергруппировка, которая, вероятно, связана с иранскими властями, угрожает расправой экспертам из компании Trend Micro. В ходе изучения сервера, который имеет отношение к вероятной утечке информации в одной из ближневосточных стран, эксперты получили сообщение, содержащее призыв остановить исследование и угрозу убийства.

Упомянутый сервер применяется кибергруппировкой MuddyWaters и выступает в качестве ее командной инфраструктуры. Используя ее, хакеры атаковали ряд правительственных организаций в ближневосточных и центральноазиатских странах…

Специалисты Trend Micro нашли этот сервер в рамках расследования инцидента с применением фишинговых писем с вредоносным вложенным файлом…» ***(Хакеры из Ирана угрожают расправой экспертам в сфере информационной безопасности // SecureNews (https://securenews.ru/iranian_hackers_2/). 14.03.2018).***

***

«Неизвестные хакеры путем прямого компьютерного взлома похитили в Японии в 2017 году криптовалюты на 662,4 млн иен ($6,3 млн). Об этом сообщило в четверг Главное полицейское управление страны, которое впервые публикует такую статистику.

Всего, по этим данным, в прошлом году было зафиксировано 149 краж криптовалюты путем компьютерного взлома…

В то же время крупнейшей в мире преступной акцией с криптовалютой остается пока еще до конца не раскрытое похищение криптовалюты NEM на сумму 58 млрд иен (около $548 млн) с японской криптовалютной биржи Coincheck. По предварительным данным, она была осуществлена в минувшем январе не путем взлома, а с помощью заражения компьютеров служащих биржи специально разработанным вирусом.

По данным расследования, вирус попал в систему через сообщение электронной почты. 12 марта биржа Coincheck провела выплату компенсаций своим клиентам, пострадавшим от кражи. Их получили примерно 260 тыс. человек. Всего им выплачено в примерно 46,6 млрд иен (более $437 млн).

С февраля в Японии проходят тотальные проверки всех криптовалютных бирж…» ***(В Японии в 2017 году хакеры похитили криптовалюты на $6,3 млн // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5486321-V-Yaponii-v-2017-godu-xakery-poxiti.html#ixzz5AsAArQ2I). 22.03.2018).***

***

«…22 марта официальный сайт Министерства обороны РФ был атакован хакерами во время финального голосования за названия новейших отечественных вооружений, которое проходило на данном ресурсе.

В течение дня киберпреступники семь раз осуществляли атаку на интернет-портал Минобороны. Пять атак имели среднюю мощность, но последние два

инцидента, которые были зафиксированы с 19:00 до 20:00 по Москве, стали наиболее масштабными. Хакеры атаковали с территории стран Западной Европы, а также Украины и США. Экспертам в сфере компьютерной безопасности удалось успешно их отразить…» ***(Хакеры осуществили атаку на Министерство обороны России // SecureNews (https://securenews.ru/minoborony_rf/). 23.06.2018).***

***

«…По данным компании Group-IB, 26 марта Cobalt организовала фишинговую рассылку от имени некоммерческой организации SpamHaus, которая борется со спамом. Изучив структуру атаки, специалисты Group-IB пришли к выводу, за рассылкой стоит именно Cobalt.

В Испании арестовали лидера хакерской группировки Cobalt, похитившей более 1 млрд евро примерно у 100 финансовых организаций по всему миру, сообщили в Европоле. По информации Group-IB, лидер Cobalt является гражданином России…» ***(В Group-IB зафиксировали новую атаку хакерской группы Cobalt // «Открытые системы» (https://www.computerworld.ru/news/V-Group-IB-zafixirovali-novuyu-ataku-hakerskoy-gruppy-Sobalt). 27.03.2018).***

***

«Дані близько 150 млн користувачів сайту і мобільного застосування за підрахунком калорій MyFitnessPal були вкрадені хакерами. Про це повідомило агентство Reuters з посиланням на американського виробника спортивного екіпірування Under Armour…

За його інформацією, крадіжка сталася ще в лютому. Зловмисникам вдалося викрасти імена користувачів, електронні адреси та зашифровані паролі, однак номера водійських прав, карток соціального страхування, а також дані платіжних карт не були скомпрометовані. Однак, в Under Armour не пояснили, яким чином став можливим подібна витік.

На даний момент Under Armour співпрацює з фірмами, що працюють у сфері безпеки даних, а також з правоохоронними органами…. Всіх користувачів сайту MyFitnessPal вже повідомили про інцидент і попросили поміняти паролі.

Як додає Reuters, це найбільший витік даних в цьому році і одна з наймасовіших за весь час…» ***(Самуїл Проскуряков. Дані близько 150 млн користувачів додатка MyFitnessPal вкрадені хакерами // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1722695-dani-blizko-150-mln-koristuvachiv-dodatka-myfitnesspal-vkradeni-khakerami). 30.03.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«Спустя три недели после удаления опасного «банковского» приложения "Универсальный мобильный банкинг", которое воровало данные платежных

карт украинцев, в сервисе Google Play появился его клон – идентичное приложение «Универсальный банкинг»...

Новое приложение полностью идентично по функционалу и оформлению своему «старшему коллеге»: позиционирует себя как реализатор функций мобильного банкинга пяти отечественных финансовых учреждений (ПриватБанк, Ощадбанк, ОТП-Банк, Альфа-Банк, Райффайзен Банк Аваль). После установки также запрашивает логин и пароль к действующим легитимным мобильным банковским сервисам, а потом – и пин-код от банковской карты. Более того, осталось даже старое название вредоносного приложения: при установке «Универсального банкинга» устройство идентифицирует его как «Универсальный мобильный банкинг»…

Разработчиком «нового» приложения выступает «GroupU» вместо «universal»…» ***(Владимир Кондрашов. В Google Play опять появилось банковское приложение, ворующее деньги украинцев // InternetUA (http://internetua.com/v-google-play-opyat-poyavilos-bankovskoe-prilojenie-voruuasxee-dengi-ukraincev). 13.03.2018).***

***

«…Эксперты по кибербезопасности отмечают, что вредоносные майнеры теперь могут «убивать» процессы запущенных программ-конкурентов в оперативной памяти. Это позволяет им получить полный и единоличный контроль над всеми ресурсами компьютера.

Ксавье Мартенс, специалист по кибербезопасности из ICS Sans, пояснил, что изученный им модифицированный майнер почти не отличался от «коллег по опасному бизнесу». Единственным исключением была функция Kill List, позволяющая вредоносной программе завершать работу конкурентов.

Создатель «программы-киллера» пошёл на этот шаг из-за того, что найти не заражённый майнером компьютер всё сложнее, поэтому, внедрив в своё детище новую функцию, он обеспечил ему существенное преимущество.

Мартенс уверен, что автор майнера-киллера сделал большую работу, результаты которой можно применить для разработки противовирусного ПО, позволяющего эффективно и сразу «убивать» все приложения, добывающие криптовалюту на чужих компьютерах без ведома владельцев…» ***(Вячеслав Ларионов. Вирусы-майнеры научились устранять конкурентов // Hi-News.ru (https://hi-news.ru/technology/virusy-majnery-nauchilis-ustranyat-konkurentov.html). 07.03.2018).***

***

«Check Point Software Technologies опубликовала отчет Global Threat Impact Index, согласно которому от незаконной добычи криптовалюты в феврале пострадало 42% компаний во всем мире.

Исследователи Check Point выявили три различных варианта вредоносных криптомайнеров, которые вошли в топ-10 активных зловредов…

Самые активные зловреды февраля 2018:

Coinhive — зловред, предназначенный для добычи криптовалюты Monero без ведома пользователя, когда тот посещает веб-сайты.

Cryptoloot — криптомайнер, использующий мощность ЦП или видеокарты жертвы и другие ресурсы для майнинга криптовалюты, зловред добавляет транзакции в блокчейн и выпускает новую валюту.

Rig ek — набор эксплойтов, который появился в 2014 году. Rig включает эксплойты для Internet Explorer, Flash, Java и Silverlight…

Самые активные мобильные зловреды февраля 2018:

Triada — модульный бэкдор для Android, который дает огромные привилегии скачанным зловредам.

Lokibot — банковский троян для Android, который крадет пользовательские данные и требует за них выкуп. Зловред может заблокировать телефон, если удалить его права администратора.

Hiddad — зловред для Android, который переупаковывает легитимные приложения и затем реализует их в магазинах сторонних производителей…» ***(Check Point: глобально 42% компаний пострадали от криптомайнинга // «Компьютерное Обозрение» (http://ko.com.ua/check_point_globalno_42_kompanij_postradali_ot_kriptomajninga_123884). 15.03.2018).***

***

«Исследователи из MalwareHunterTeam обнаружили вторую версию нашумевшего шифровальщика GandCrab, улучшенную и доработанную авторами.

…Во-первых, поменялись имена командных серверов, с которыми связывается вымогатель перед шифрованием файлов…

Хосты теперь выглядят следующим образом:

politiaromana.bit

malwarehunterteam.bit

gdcb.bit

Во-вторых, изменилось расширение, которое зловред присваивает зашифрованным документам. Если первая версия создавала GDCB-файлы, то новая дает на выходе образцы вида test.jpg.CRAB…

Записка с требованием выкупа теперь называется не GDCB-DECRYPT, а CRAB-Decrypt. В ней содержатся не только инструкции по переходу на сайт в onion-домене, но и ссылка на Tox-чат для тех, кто не может установить браузер Tor.

Еще одно отличие относится к внешнему виду сайта с руководством по уплате выкупа: на странице появился список порталов, где жертва может купить криптовалюту DASH, и QR-код, сменивший ссылку на кошелек мошенников…

О новой версии GandCrab его создатели впервые упомянули после того, как в Сеть выложили бесплатный декриптор для первого выпуска вредоноса. Киберпреступники пообещали усилить защиту командных серверов и сделать свое детище менее доступным для взлома. Свои обещания они сдержали: дешифровать GandCrab v2 с помощью захваченных ключей пока нельзя…» ***(Julia Glazova. GandCrab эволюционировал и не поддается дешифровке // Threatpost***

(https://threatpost.ru/gandcrab-evolved-and-is-no-more-decryptable/24936/). 07.03.2018).

***

«…В открытом доступе появились первые PoC-коды, облегчающие проведение мощнейших атак с memcached-плечом.

Один из этих инструментов, по свидетельству Bleeping Computer, представляет собой написанный на Python скрипт, позволяющий с помощью Shodan выявлять доступные из Интернета memcached-серверы и в считаные секунды организовывать DDoS-атаку на выбранную мишень. Как оказалось, этот PoC, именуемый Memcrashed, создал ИБ-исследователь Амир Мохаммади (Amir Khashayar Mohammadi).

Вторая утилита для автоматизации memcached-атак была выложена на Pastebin пятого марта анонимом. Этот скрипт написан на C и предлагается в комплекте со списком из более 17 тыс. IP-адресов, пригодных для использования в качестве «отражателей» DDoS-трафика.

Третий PoC, по свидетельству репортера, настолько мал, что уместился в сообщении, опубликованном в Twitter…

Комментируя публикацию PoC-кодов, глава некоммерческой ИБ-организации GDI Foundation Виктор Геверс (Victor Gevers) отметил, что они предупреждают владельцев memcached-серверов о возможности злоупотреблений уже почти два года, советуя усилить защиту и помещать такие устройства за межсетевым экраном…

Выступая в прошлом году на конференции, эксперты Qihoo 360 тоже предупредили о возможности использования memcached-серверов в атаках… Первые memcached-атаки Qihoo 360 зафиксировала 24 февраля, и за десять последующих дней исследователи насчитали около 15 тыс. таких DrDoS, более 7 тыс. мишеней и до 20 612 memcached-участников атаки.

Чтобы уберечь свою инфраструктуру от злоупотреблений, многие поставщики облачных услуг уже начали ограничивать скорость передачи данных, отправляемых с UDP-порта 11211. Владельцы memcached-серверов тоже, наконец, вняли увещеваниям ввиду реальности угрозы: Rapid7 сообщает о резком сокращении числа серверов с открытым портом 11211, то же самое наблюдает Геверс.

Тем временем для жертв DrDoS с новым вектором появилась возможность самостоятельно остановить атаку. Один из разработчиков memcached-сервера, использующий псевдоним Dormando, предложил отправлять атакующим команды shutdown и flush_all. Первая принудительно завершает работу системы , вторая очищает кэшируемую память сервера, в том числе от вредоносных пакетов…

Опубликовавший PoC-код Мохаммади тоже внес свою лепту в создание противоядия — написал Python-утилиту, позволяющую автоматизировать отправку команд flush_all и shutdown источникам вредоносных пакетов. Инструмент, нареченный Memfixed, уже выложен на GitHub…

Кураторы проекта Memcached, со своей стороны, позаботились об исправлении ошибки конфигурации (CVE-2018-1000115) и выпустили обновление

1.5.6, отключающее UDP по умолчанию…» ***(Maxim Zaitsev. DDoS с участием memcached: PoC-коды и противоядие // Threatpost (https://threatpost.ru/memcached-ddos-poc-codes-and-antidote-published/24943/). 12.03.2018).***

***

«Исследователи компании Palo Alto Networks обнаружили новый зловред для Windows, целью которого является похищение криптовалюты и перехват цифровых платежей.

…Троянец ComboJack способен идентифицировать адреса цифровых кошельков, скопированные пользователем Windows в буфер обмена, и подменять их адресами кошельков организаторов атаки. Соответственно, осуществляя транзакцию, пользователь вставляет не тот адрес, который скопировал – и деньги переводятся киберпреступникам.

Троянец распространяется в фишинговых сообщениях электронной почты, замаскированный под вложение в формате PDF. В случае его загрузки и открытия автоматически открывается еще и файл RTF со встроенным HTA приложением, которое эксплуатирует уязвимость CVE-2017-8579 в DirectX… ComboJack… способен выявлять и подменять адреса для транзакций в криптовалютах Bitcoin, Litecoin, Ethereum и Monero, а также в платежных системах Qiwi, Yandex Money и WebMoney» ***(Копипейст с сюрпризом // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5479846-Kopipejst-s-syurprizom.html#ixzz5ABvYG27s). 12.03.2018).***

***

«…В сентябре 2017 года в Google Play появилось приложение Monero Miner (XMR) разработчика My Portable Software…

В отличие от известных лжемайнеров, …Monero Miner действительно добывал криптовалюту. Проблема в том, что все средства поступали разработчику, вне зависимости от того, какой адрес кошелька указывал пользователь во время настройки приложения.

Несмотря на низкий рейтинг и негативные отзывы, приложение установили до 50 000 пользователей. После предупреждения специалистов ESET майнер был удален из Google Play…

ESET рекомендует загружать мобильные приложения для майнинга, предварительно изучив число загрузок, оценки и отзывы других пользователей…» ***(Обнаружена новая афера с криптовалютами // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5480063-Obnaruzhena-novaya-afera-s-kriptova.html#ixzz5ABxAAKuq). 13.03.2018).***

***

«В фармацевтических компаниях Вьетнама обнаружены следы вредоносного ПО PlugX…

PlugX – инструмент удалённого контроля, крайне популярный среди организаторов сложных целевых атак и кампаний кибершпионажа…

PlugX использовался целым рядом китайскоговорящих кибергруппировок, включая Deep Panda, NetTraveler и Winnti…

PlugX позволяет атакующим удалённо выполнять различные вредоносные операции в системе без разрешения пользователя, например, копировать и модифицировать файлы, запоминать нажатия клавиш, воровать пароли, делать снимки экрана. Таким образом, злоумышленники могут незаметно собирать и красть конфиденциальную информацию из заражённой системы...» ***(Китайскоговорящие хакеры заинтересовались фармацевтикой // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5480673-Kitajskogovoryashhie-xakery-zainter.html#ixzz5AC2W0QZo). 15.03.2018).***

***

«Специалисты компании Avast выявили новую методику распространения криптовалютных майнеров. Как утверждают эксперты, хакеры добавляют код вредоносного программного обеспечения в копии проектов на портале GitHub.

«Ответвления» проектов (fork) на Github – это копии чужих проектов, содержащих некоторые изменения. Сейчас хакеры создают форки случайных проектов, а затем внедряют вредоносные файлы в структуру каталогов.

Пользователи могут не загружать вредоносные исполняемые файлы напрямую с GitHub. Вместо этого распространение вредоносного ПО через фишинговую кампанию. По словам экспертов, файл загружается при посещении пользователем сайта, на котором размещено фишинговое рекламное объявление, и если жертва кликает по одному из таких баннеров.

После клика по рекламному объявлению на компьютер пользователя осуществляется установка вредоносной программы, замаскированной под обновление для Adobe Flash Player. Его загрузка производится с GitHub, где размещен код вредоносной программы, спрятанный в копиях проектов.

Кроме того, данная программа осуществляет установку вредоносного расширения Chrome, которое показывает рекламные объявления в фоновом режиме и кликает по ним, что дает возможность хакерам получать более существенную прибыль из вредоносной кампании…

Сейчас администрация ресурса ведет активную работу с Avast по удалению вредоносных копий проектов…» ***(Хакеры скрывают криптовалютные майнеры в проектах на GitHub // SecureNews (https://securenews.ru/github_6/). 16.03.2018).***

***

«Китайские хакеры пользуются вредоносной программой RottenSys для организации ботнета, который уже состоит из 5000000 Android-устройств.

Вредоносная программа применяется для демонстрации навязчивой рекламных объявлений на экране инфицированных устройств. Однако эксперты Check Point выявили факты использования экспертами нового модуля, написанного на языке Lua и предназначенного для объединения инфицированных устройств в одну гигантский ботнет.

Как утверждают исследователи, ботсеть дает киберпреступникам гораздо больше возможностей, чем простой показ рекламных объявлений. Так, она сможет скрытно осуществлять установку дополнительных приложений и автоматизацию пользовательского интерфейса…

Компонент на Lua, который позволяет операторам ботсети захватывать контроль над инфицированными устройствами, был внедрен в RottenSys лишь в минувшем месяце. На данный момент вредоносная программа активна лишь на китайском рынке и ее распространение осуществляется посредством китайских зараженных приложений. Ботнет в большинстве своем состоит из устройств Huawei, Xiaomi, OPPO, vivo, LeEco, Coolpad и GIONEE.» ***(Хакеры из Китая организовали ботсеть из 5000000 Android-устройств // SecureNews (https://securenews.ru/rottensys/). 16.03.2018).***

***

«Эксперты из Forcepoint сообщили о новой киберкампании с использованием троянской программы Qrypter.

Эта вредоносная программа существует на протяжении уже нескольких лет и была разработана хакерской группой QUA R&D…

Qrypter (Qarallax, Qontroller, QRAT, Quaverse) – это троянская программа для удаленного доступа на базе Java, которая работает с командными серверами на основе Tor…

Распространение вредоносной программы осуществляется посредством электронной почтовой рассылки…

Qrypter предоставляет хакерам большой арсенал возможностей: можно подключаться к удаленному рабочему столу, получать доступ к веб-камерам, манипулировать файловой системой, устанавливать дополнительные файлы и управлять диспетчером задач.

Ежемесячная стоимость аренды троянской программы составляет 80 долларов. Заплатить за услугу можно с помощью Bitcoin, Bitcoin-Cash и PerfectMoney. Кроме того, со скидкой можно приобрести подписку на три месяца или год…» ***(Троянская программа Qrypter атакует организации по всему миру // SecureNews (https://securenews.ru/qrypter/). 15.03.2018).***

***

«Фахівці з кібербезпеки повідомили про атаку нового вірусу, який здатний вкрасти файли і доступ до облікових записів користувачів. Подробиці опублікували експерти компанії Dr.Web у своєму блозі.

Вірус в модифікаціях Trojan.PWS.Stealer.23012 і Trojan.PWS.Stealer.23198 робить скріншоти екрану і копіює з комп'ютера текстові файли та зображення, а також логіни та паролі, збережені в браузерах. Отриману інформацію він зберігає в архів і висилає зловмисникам…

Шкідливе програмне забезпечення поширюється через посилання в коментарях на YouTube під виглядом корисних додатків і путівників по чит-ходам у комп'ютерних іграх. Щоб переконати користувачів завантажити вірус з файлообмінника, зловмисники супроводжують посилання схвальними

коментарями, написаними від імені підроблених записів. Уразливими виявилися всі комп'ютери на платформі Windows…» ***(На YouTube виявили новий вірус, який краде файли // ТзОВ "Редакційні системи" (http://expres.ua/news/2018/03/24/288900-youtube-vyyavyly-novyy-virus-krade-fayly). 24.03.2018).***

***

«Эксперты по безопасности компании Palo Alto Networks выявили новую вредоносную программу для Android, которая использует API для ботов в Telegram для связи с контрольным сервером (C&C) и вывода данных с устройства жертвы.

«Боты» в Telegram это специальные аккаунты, используемые, как правило, для подтягивания контента со сторонних сервисов или для отправки пользователям специализированных уведомлений и новостей.

TeleRAT …атакует иранских пользователей, маскируясь, в том числе, под приложения, которые позволяют индексировать количество просмотров профиля в Telegram…

TeleRAT создает и заполняет два файла - telerat2.txt (включающий всевозможные данные об устройстве - версию системного загрузчика, доступную память и количество процессорных ядер) и thisapk_slm.txt (содержит информацию о канале Telegram и список команд). После установки в системе вредонос уведомляет об этом злоумышленников, отправляя боту сообщение с текущей датой и временем.

После этого запускается фоновый процесс, который раз в 4,6 секунды проверяет поступление новых команд (передаваемых на языке фарси).

Вредонос способен получать (и передавать) информацию о контактах, местоположении, списке приложений, содержимом буфера обмена. Кроме этого он способен загружать файлы, создавать новые контакты, устанавливать обои, получать и отправлять SMS, делать фотографии фотографий и управлять звонками…

В коде TeleRAT эксперты нашли имя разработчика, которое привело их к каналу Telegram ‘vahidmail67’. Этот канал занимается рекламой всевозможных сомнительных приложений, от накрутчиков для Instagtam до шифровальщиков-вымогателей. Нашлись также ссылки на программерские форумы в Иране, где продавалась библиотека средств управления ботами в Telegram…» ***(Трояны научились воровать данные с помощью Telegram // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5487031-Troyany-nauchilis-vorovat-dannye.html#ixzz5As8GAMZn). 26.03.2018).***

***

«Компанію Boeing атакували вірусом, схожим на WannaCry…

Видання The New York Times цитує повідомлення, розіслане співробітникам Boeing головним інженером департаменту комерційних літаків Майком Вандервелом, в якому йдеться, що вірус поширюється «ніби метастази».

Існує небезпека, що вірус вразить виробничі системи Boeing і програмне забезпечення літаків, пише Вандервел.

Авіаконцерн ввечері 28 березня за місцевим часом поширив заяву, в якій визнав факт кібератаки, але підкреслив, що вона має локальний характер і була зупинена.

Подробиці кібератаки, в тому числі передбачуване використання вірусу WannaCry або подібного йому, у Boeing поки розкривати відмовилися.» ***(Авіаконцерн Boeing потерпає від кібератаки // Західна інформаційна корпорація (https://zik.ua/news/2018/03/29/aviakontsern_boeing_poterpaie_vid_kiberataky_1295065). 29.03.2018).***

***

«Группа экспертов по кибербезопасности MalwareHunterTeam обнаружила новую программу-вымогатель AVCrypt, блокирующую работу установленных на компьютере антивирусов.

… AVCrypt не только лишь пробует удалить антивирусные программы перед шифрованием файлов жертвы, однако и устраняет некоторые службы Windows. Затем программа делает запрос об антивирусах, которые зарегистрированы в Центре обеспечения безопасности платформы.

Также новинка осуществляет попытку освободиться от них через использование командной строки… Исследователи в области информационной безопасности отмечают, что никогда раньше не фиксировали деятельность вымогателей такого рода.

Они также предположили, что вирус может являться программой-вайпером, то есть создан для уничтожения информации на устройстве жертвы. Специалисты отметили, что злоумышленники не оставили контактные данные для отправки выкупа. Вместо этого в записке с требованиями они написали «lol n» ***(Обнаружен новый вирус-вымогатель, удаляющий антивирусы // ПРОЕКТ УКРАИНСКИЙ ВЫБОР(http://vybor.ua/news/world_news/obnarujen_novyy_virus_vymogatel_udalyayushchiy_antivirusy.html). 29.03.2018).***

***

«…Компания Trend Micro, специализирующаяся в сфере кибербезопасности, сообщает о новом типе вредоносного ПО для Android.

Внедренный хакерами майнер будет добывать Monero используя процессор смартфона до тех пор, пока не исчерпает все ресурсы или мобильное устройство не сломается.

В коде HiddenMiner нет контроллера, переключателя или оптимизатора, он постоянно майнит Monero, вплоть до перегрева мобильного устройства…

HiddenMiner представляет собой приложение в Google Play и заставляет пользователей активировать его в качестве администратора устройства.

Он будет постоянно появляться, пока жертвы не нажмут кнопку «Активировать»; после предоставления разрешения HiddenMiner начнет добывать Monero в фоновом режиме, предупреждает Trend Micro.

Удалить майнер трудно, он блокирует такие действия пользователя» ***(Вредоносная программа будет майнить Monero на вашем смартфоне, пока он не сломается // BIGFIN (https://bigfin.net/29/03/2018/vredonosnaja-programma-budet-majnit-monero-na-vashem-smartfone-poka-on-ne-slomaetsja/). 29.03.2018).***

***

«Специалисты по кибербезопасности из компании Cisco Talos обнаружили новый вирус, который избирательно атакует машины, работающие на системе Lunix. «Умный» инструмент был назван GoScanSSH.

…он написан на языке программирования Go и ищет уязвимые серверы для удаленного доступа. В первой серии атак киберпреступники прописывали алгоритм нападения буквально вручную, используя более семи тысяч комбинаций пар логинов и паролей.

Они были нацелены на слабо защищенные учетные записи. При успешном подборе пароля система заражалась.

Разработчики специально прописали код таким образом, чтобы вредоносное программное обеспечение избегало военных и правительственных сетей…

Специалисты пока не могут точно ответить на вопрос о предназначении вируса. Его механизм, по мнению экспертов, похож на принудительный майнер криптовалюты, однако пока зараженные машины не были замечены в подобных действиях...» ***(Неопознанный вирус пощадил чиновников и военных // Goodnews.ua (http://goodnews.ua/technologies/neopoznannyj-virus-poshhadil-chinovnikov-i-voennyx/). 29.03.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Национальная жандармерия Франции совместно с Европолом положила конец преступной организации, промышлявшей масштабным корпоративным мошенничеством. По данным правоохранительных органов, злоумышленники действовали на территории от Франции до Гонконга, и ущерб от их преступлений составил 4,6 миллиона евро.

Расследование началось в июне 2016 года, когда французские полицейские обнаружили два случая CEO-мошенничества…

В рамках этой схемы преступники отправляют сотруднику организации письмо якобы от генерального директора и просят срочно провести некий платеж. Злоумышленники рассчитывают, что работник постарается побыстрее выполнить просьбу начальника…

Атаке предшествует длительная подготовка — преступники изучают, как устроена компания, и регистрируют домен, похожий на корпоративный…

В случае французских аферистов речь идет как минимум о 24 атаках, которые принесли преступникам 4,6 млн евро. Поддельные компании и банковские счета

для них открывали 15 граждан Румынии, проживавших во Франции и Бельгии. Еще двое мошенников с гражданством этих стран подбирали персонал и регистрировали юридические и нотариальные конторы с румынскими реквизитами. Через эти фирмы-прослойки украденные средства попадали в Гонконг.

Помимо французских правоохранителей, в расследовании приняли участие следователи и эксперты из Бельгии, Румынии, Израиля и Швейцарии…» ***(Julia Glazova. Международная кибергруппировка украла почти 5 млн евро // Threatpost (https://threatpost.ru/ceo-fraudsters-got-arrested-in-france/24921/). 06.03.2018).***

***

«Российский гражданин, который в июле 2017 года предстал перед американским судом по делу о масштабных киберпреступлениях, пошел на сделку с правосудием и частично признал свою вину.

Правоохранительные органы утверждают, что Юрий Мартышев и его сообщник Руслан Бондарь стоят за Scan4You — популярным в «темном» Интернете сервисом проверки зловредного ПО на обнаружение антивирусными движками.

Согласно судебным документам, обвиняемые вели преступную деятельность в 2009–2017 годах. За плату в 15 центов они предлагали вирусописателям загрузить свои разработки на сайт, чтобы узнать, сможет ли вредонос обойти популярные защитные системы. Всего за эти годы сервисом Scan4You воспользовались тысячи клиентов, которые протестировали миллионы файлов.

В своем заявлении Мартышев рассказал, что среди них были организаторы масштабной кибератаки на некоего крупного ритейлера, которая состоялась в 2013 году. Эксперты полагают, что речь идет о взломе Target, когда преступники украли данные 40 млн платежных карт и персональные данные 70 млн покупателей…

Мартышев также отметил, что их услугами воспользовался ботовод Citadel. Ущерб от активности этой бот-сети оценивается в 500 млн долларов — эти деньги мошенники смогли украсть с банковских аккаунтов по всему миру…

Летом 2017 года Мартышева арестовали в Латвии и экстрадировали в США, где ему теперь грозит десятилетний срок и штраф в размере не менее 250 тыс. долларов. Он признал себя виновным по двум из четырех пунктов обвинения в кибермошенничестве — преступном сговоре и соучастии в компьютерном взломе.

…Мартышев также выплатит более 125 тыс. долларов в качестве компенсации ущерба и передаст правоохранительным органам все программно-аппаратные средства, которые он использовал с преступными целями…» ***(Julia Glazova. В США судят российского гражданина за киберпреступления // Threatpost (https://threatpost.ru/russian-cybercriminal-pleads-guilty-in-us/25031/). 16.03.2018).***

***

«Как сообщает пресс-служба МВД России, правоохранители остановили деятельность группы мошенников, которые занимались кражей средств с

банковских карт, используя вредоносную программу, замаскированную под безобидные Android-приложения.

В материалах дела указано, что 19-летний житель Санкт-Петербурга осуществил разработку нескольких безобидных Android-программ. Но в эти программы был внедрен вредоносный код, который давал возможность красть деньги с платежных карт, а также осуществлять перехват SMS-сообщений с паролями для организации переводов средств и уведомления о списании.

В пресс-службе МВД России подчеркнули, что мошенники похищали не более чем 8000 рублей с одной карты. Это сумма является суточным лимитом на операции по переводу.

От действий злоумышленников пострадали жители Архангельской, Иркутской, Ленинградской и Московской областей, а также Чеченской Республики. Похищенные средства переводились на разные счета в Братске, где их обналичивал местный житель, ранее имевший несколько судимостей. Сейчас в отношении хакеров заведено уголовное дело.» ***(Хакер из Санкт-Петербурга занимался кражей средств с банковских карт // SecureNews (https://securenews.ru/spb/). 16.03.2018).***

***

«Полиция Испании задержала гражданина Украины, который занимался взломом банкоматов и организовал атаки на сотни банков в России, сообщил глава испанского МВД Хуан Игнасио Соидо...

«Хакерские атаки совершались на почти все российские банки», – добавил Соидо.

Речь идет об атаках на порядка 300-400 кредитных организаций в России. Из крупных банков не был атакован только Сбербанк. При этом из 50 российских банков были похищены деньги. Подчеркивается, что главной целью злоумышленников были именно российские банки, хотя атаки распространялись и на другие страны.

Задержанный гражданин Украины (инициалы Денис К) ранее отбывал наказание в России. В 2014 году из Украины он приехал в испанский город Аликанте. В настоящее время его заключили под стражу, дело в отношении украинца передадут в национальный суд. Пока вопрос об экстрадиции не стоит.

Кроме Дениса К. организаторами атак были еще трое человек – граждане Украины и России…

После атак деньги переводили в криптовалюту. Среднюю сумму каждой атаки правоохранительные органы Испании оценивают в 1,5 млн долларов.

Помимо России атаки совершались в Белоруссии, Азербайджане, Казахстане, на Украине и Тайване. В 2017 году хакеры совершали атаки на банкоматы в Мадриде на общую сумму в 500 тыс. евро.

Отмечается, что всего правоохранителям удалось идентифицировать 15 членов группировки.

Задержали гражданина Украины в начале марта сотрудники Национальной полиции Испании. Отмечается, что в расследовании также принимали участие ФБР, Европол, МВД Белоруссии, Азербайджана и Тайваня…» ***(Антон Касс.***

Задержан украинец, организовавший атаки на сотни российских банков // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/3/26/914375.html). 26.03.2018).

***

«Чехия выдала США россиянина Евгения Никулина, обвиняемого американскими судебными властями в хакерских атаках и краже информации с компьютеров компаний LinkedIn и Dropbox…

Е.Никулин был арестован чешскими властями при сотрудничестве с ФБР в октябре 2016 года. Тогда в Белом доме заявили, что США серьезно относятся к проблеме кибербезопасности и будут защищать свои интересы. В министерстве юстиции США сообщили, что дело хакера засекречено.

В конце ноября 2017 года Верховный суд в Праге одобрил возможность экстрадиции Е.Никулина в США…

Американская компания LinkedIn сообщила, что арест в Чехии гражданина РФ имеет отношение к расследованию дела о кибернападении на LinkedIn в 2012 году…» ***(Чехия выдала США россиянина, обвиняемого в хакерских атаках // Interfax-Azerbaijan (http://interfax.az/view/729421). 30.03.2018).***

***

Технічні аспекти кібербезпеки

«Zurich объединился с Citigroup и Depository Trust & Clearing Corporation (DTCC) для разработки стандартов кибербезопасности технологических компаний с целью противодействия бэкдор-атакам…

Согласно сообщению The Financial Times, крупные банки, страховщики и другие финансовые учреждения активно занимаются укреплением своей киберзащиты, но то же самое нельзя сказать о небольших компаниях, которые разрабатывают нишевые продукты (онлайн-кредитование, платежи, управление капиталом и биометрия).

Многие крупные финансовые учреждения вступили в партнерские отношения с такими компаниями, позволяя им обрабатывать и хранить данные клиентов. Это делает уязвимой вершину финансового сектора.

Консорциум обязался разработать набор стандартов кибербезопасности после встречи, на Всемирном экономическом форуме в Давосе…

Ожидается, что стандарты будут реализованы в течение следующих шести-двенадцати месяцев» ***(Стандарты кибербезопасности разработают Zurich, Citigroup и DTCC // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/standartyi-kiberbezopasnosti-razrabotayut-zurich-citigroup-i-dtcc). 07.03.2018).***

***

«…Развитие технологий искусственного интеллекта поможет победить в кибервойнах будущего, заявил на конференции «Искусственный интеллект: проблемы и пути решения» заместитель министра обороны Юрий Борисов…

По его мнению, у России с ее сильной математической школой «есть все возможности», чтобы стать лидером в этой области…

Борисов считает, что …человечество подходит к новой эпохе, когда становится недостаточно просто быстрых вычислений, для обработки и хранения терабайтов информационных потоков нужны интеллектуальные системы…» ***(Минобороны зовёт на помощь искусственный интеллект для победы в кибервойне // РосКомСвобода (https://roskomsvoboda.org/37087/). 14.03.2018).***

***

«…На прошлой неделе исследователи из Citizen Lab обнаружили, что устройства PacketLogic от компании Sandvine использовались для захвата незашифрованных интернет-подключений пользователей. Этот случай является еще одной хорошей демонстрацией важности шифрования сети с помощью протокола HTTPS. Турецкие и сирийские пользователи, пытавшиеся загрузить официальные приложения, вместо этого неосознанно устанавливали вредоносное ПО, предназначенное для слежки за ними. В Египте эти устройства вводили контент, направленный на зарабатывание денег, в веб-трафик пользователей, в том числе рекламные и криптовалютные скрипты.

Это стандартные кибератаки по схеме “человек посередине” (MITM), в рамках которых компьютер на пути между вашим браузером и официальным веб-сервером способен перехватывать и изменять трафик. Это может произойти, если ваши веб-соединения используют стандартный протокол HTTP, поскольку данные, передаваемые по HTTP, не шифруются и могут быть изменены или прочитаны кем угодно в сети.

Модули Sandvine работали как раз по такой схеме…

Администраторы сайтов могут снизить число и последствия таких атак, используя HTTPS вместо HTTP…

Такие программные решения, как Let‘s Encrypt и Certbot упрощают развертывание веб-сайтов под HTTPS и обеспечивают защищенный доступ к контенту. В текущем году Google Chrome планирует отмечать все HTTP-сайты как “небезопасные”. Сегодня почти 80% веб-трафика в США зашифровано с помощью протокола HTTPS…» ***(Тотальная слежка и кибератаки ускоряют массовый переход на протокол HTTPS // РосКомСвобода (https://roskomsvoboda.org/37064/). 14.03.2018).***

***

«…Эксперты по кибербезопасности в общей сложности заработали $267 тыс. в рамках хакерского соревнования Pwn2Own 2018 за взлом Microsoft Edge, Apple Safari, Oracle VirtualBox и Mozilla Firefox.

В первый день исследователь Ричард Чжу (Richard Zhu), известный под псевдонимом fluorescence, не смог взломать браузер Safari, однако продемонстрировал атаку с использованием цепочки эксплоитов для браузера Edge, которая принесла ему $70 тыс. Никлас Баумстарк (Niklas Baumstark) из команды Phoenhex получил $27 тыс. за взлом программного обеспечения

VirtualBox, а Самуель Грос (Samuel Groß), известный под псевдонимом saelo, заработал $65 тыс. за взлом Safari.

Во второй день Pwn2Own 2018 Чжу заработал $50 тыс. за взлом Firefox, проэксплуатировав уязвимость чтения за пределами поля (out-of-bounds) и целочисленного переполнения в ядре Windows…

Сотрудники Ret2 Systems продемонстрировали цепочку эксплоитов для Safari, однако успешно взломать браузер удалось только с четвертой попытки…

Pwn2Own – соревнование хакеров, которое ежегодно проводится в рамках конференции по информационной безопасности CanSecWest, начиная с 2007 года. Во время проведения конкурса участники ищут ранее неизвестные уязвимости в общедоступном и популярном ПО, а также в популярных мобильных устройствах…» ***(Исследователи заработали $267 тыс. в рамках Pwn2Own 2018 // SecurityLabRu (https://www.securitylab.ru/news/492164.php). 16.03.2018)***.

***

«…Согласно публикации на официальном сайте, Intel исправила ошибки в прошивке некоторых старых процессорных платформ, включая Broadwell Xeon E3, Broadwell U/Y, Haswell H, S и Haswell Xeon E3. Измененные версии уже доступны производителям оборудования…

Обновления закрывают уязвимости Spectre и Meltdown, на которых основаны три сценария атак на серверные и настольные системы. …Meltdown нарушает работу механизма, который не дает приложениям обращаться к закрытым от них участкам системной памяти, а Spectre позволяет обходными маневрами считывать память других приложений…

На данный момент патчи для уязвимости Spectre для Sandy Bridge и Ivy Bridge существуют лишь в бета-версии, и сейчас они проверяются изготовителями оборудования.» ***(Lindsey O'Donnell. Новые патчи против Spectre для чипов Broadwell и Haswell // Threatpost (https://threatpost.ru/intel-releases-updated-spectre-fixes-for-broadwell-and-haswell-chips/24908/). 05.03.2018).***

***

«Ученые Венского университета (Австрия) уверены в возможности создания абсолютно защищенных каналов связи, обеспечивающих защиту не только передаваемых данных, но и самого направления их передачи. Для этого нужно передавать информацию с удвоенной скоростью света, пояснили ученые…

Благодаря необычным свойствам фотонов, запутанных на квантовом уровне, ученые заставили данные перемещаться в два раза быстрее света…

Благодаря этим свойствам фотона абонент квантовой линии способен считывать передаваемые ему данные, в то же время записывая собственные. Его абонент может читать переданные обратно данные путем сравнения свойств фотона в момент получения и в момент записи в него данных, что не противоречит теории относительности.

Ученые Венского университета даже создали специальное устройство, позволяющее осуществлять вышеописанный двусторонний обмен данными в реальном мире с помощью оптоволокна, лазеров и оптических приборов.

Передаваемые с его помощью данные шифруются автоматически, и взломать такой канал связи очень сложно. Если один из абонентов будет передавать произвольные данные, атакующий и вовсе не сможет их получить. В связи с этим подобные линии связи могут в будущем использоваться в государственных органах и финансовых организациях…» ***(Физикам удалось передать информацию с двойной скоростью света // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=121941). 14.03.2018).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«…знаменитого голосового помощника в Windows 10 от Microsoft – Кортану – можно использовать в качестве своего рода проводника к взлому любого компьютера с данной операционной системой, даже если тот заблокирован. Это сумели доказать израильские специалисты по кибербезопасности, успешно взломав операционную систему и сеть, используя функции данного голосового помощника, при этом совершенно не ощутив никакой сложности.

…совсем недавно компания Microsoft добавила возможность задействования голосового помощника Cortana даже в том случае, если экран устройства заблокирован – например, если дать ей команду зайти на тот или иной сайт, она выполнит ее, при этом минуя фактор заблокированного дисплея…

Но именно этой особенностью и воспользовались специалисты по кибербезопасности из Израиля, которые, подключив сетевой-адаптер USB к компьютеру и заставив Кортану зайти на сайт, с которого происходило скачивание вредоносных файлов. Таким образом, новая функция от Microsoft повернулась против них же самих – именно поэтому специалисты компании на данный момент заняты исправлением этой особенности, пока что, предложив редирекцию к поисковику Bing…» ***(Роман Розенталь. Cortana как инструмент в руках хакеров: найдена новая уязвимость // Faina Idea (http://www.fainaidea.com/technologii/iskusstvennyj-intellekt/cortana-kak-instrument-v-rukah-hakerov-najdena-novaya-uyazvimost-141080.html). 07.03.2018).***

***

«Израильские эксперты в области кибербезопасности обнаружили тринадцать новых типов уязвимостей в процессорах AMD Ryzen и EPYC. Все они позволяют получить доступ к защищенной области чипов, где CPU хранят важные данные, в том числе ключи шифрования и пароли. Самые критичные уязвимости получили названия Ryzenfall, Master Key, Fallout и Chimera.

Как быстро AMD сможет побороть уязвимости пока трудно сказать. Кроме того, есть опасения, что программные заплатки могут оказать негативное влияние на производительность чипсетов. На аппаратном уровне решить проблему

получится лишь в следующих поколениях процессоров…» ***(Yan Kuczinsky. В процессорах AMD обнаружена критическая уязвимость // Game2Day (https://game2day.org/news/26075/v-processorah-amd-ryzen-i-epyc-obnarujena-uyazvimost). 14.03.2018).***

***

«Компания Trustwave опубликовала результаты опроса, согласно которому организации, использующие IoT-устройства, все чаще сталкиваются с проблемами безопасности. В исследовании, проведенном для Trustwave компанией Osterman Research в ноябре 2017 года, приняли участие 137 организаций.

Как утверждают эксперты, 61% компаний, внедривших у себя технологии Интернета вещей, уже устраняли связанные с ними нарушения системы безопасности. При этом лишь у 49% опрошенных есть формальные политики и принятые процедуры установки исправлений ПО, которые помогают предотвращать атаки.

Эксперты кибербезопасности говорят о растущих рисках, связанных с Интернетом вещей, еще с 2008 года, когда маршрутизаторы стали мишенью зловреда Hydra. Однако за прошедшие 10 лет эти предупреждения по большей части ни к чему не привели.

Несмотря на все призывы к повышению безопасности Интернета вещей, 24% респондентов отметили, что их IoT-устройства уже заражались вредоносным ПО. При этом в последнее время количество атак на IoT-гаджеты выросло на 9%.

Ведущий специалист компании Trustwave по методам обеспечения безопасности Мишель Чамберленд (Michel Chamberland) считает, что большинство организаций в области защиты Интернета вещей на 10–20 лет отстает от жизни. Многие раз за разом повторяют прошлые ошибки, например, продолжают хранить свои учетные данные в виде простого текста.

Еще одна распространенная проблема — неправильно настроенные сетевые устройства. По мнению Чамберленда, количество инцидентов с использованием IoT-гаджетов, в том числе диверсий, заражений вредоносным ПО и DDoS-атак, продолжит расти…

Как показал опрос, лишь 10% организаций «совершенно» уверены в своей способности обнаружить и обезвредить нарушения системы безопасности. При этом «в некоторой степени» в этом уверены 62% компаний…

По мнению Чамберленда, обезопаситься от IoT-угроз можно при помощи нескольких простых мер. Во-первых, следует вовремя устанавливать исправления на умные устройства. Во-вторых, можно объединить такие гаджеты в отдельную сеть и постоянно их обновлять: они не должны находиться в одной среде с важными активами организации.

Согласно исследованию, лишь треть опрошенных компаний обновляют IoT-устройства в течение 24 часов после выхода исправлений…» ***(Lindsey O'Donnell. IoT-устройства: атак становится все больше // Threatpost (https://threatpost.ru/iot-security-disconnect-as-attacks-spike-device-patching-still-lags/24974/). 13.03.2018).***

***

«Компания Trustico, один из крупных продавцов SSL-сертификатов, призналась, что хранила у себя приватные ключи своих клиентов. Заявление генерального директора шокировало экспертов по кибербезопасности — теперь владельцы интернет-ресурсов, использовавшие услуги этого реселлера для формирования защищенного HTTPS-соединения, не могут быть уверены в безопасности своих данных.

Неприятное открытие последовало за попыткой Trustico отозвать 50 тысяч сертификатов, созданных на базе инфраструктуры Symantec…

В соответствии с требованиями безопасности приватный ключ должен быть известен только самому пользователю, иначе злоумышленник сможет прочитать зашифрованные с его помощью данные. Компрометация ключей интернет-ресурсов открывает возможность для атак посредника (Man-in-the-Middle), позволяя незаметно вмешиваться в коммуникацию между посетителями сайта и веб-сервером, похищать и подменять информацию…

На текущий момент нет оснований полагать, что Trustico использовала сохраненные ключи в недобросовестных целях. Тем не менее, эксперты ИБ указывают на недопустимость подобной практики…

Дополнительные опасения экспертов вызвал тот факт, что на странице с формой генерации сертификатов есть несколько различных скриптов от третьих лиц, в частности рекламные баннеры. Взлом какого-либо из них позволил бы злоумышленникам перехватывать созданные ключи, даже если бы Trustico не сохраняла их у себя…» ***(Julia Glazova. Непрофессионализм поставил под угрозу десятки тысяч сайтов // Threatpost (https://threatpost.ru/ssl-reseller-compromised-thousands-of-certificates/24891/). 02.03.2018).***

***

«Компания Cisco выпустила очередной пакет обновлений с исправлениями безопасности от марта 2018 года. В общей сложности в него попали 22 уязвимости, две из которых были классифицированы производителем как «критические».

Первая ошибка, CVE-2018-0141, связана с жестко запрограммированным паролем для приложения Cisco PCP (Prime Collaboration Provisioning)…

Стоит отметить, что по шкале оценки общих уязвимостей (CVSS) эта ошибка получила всего 5,9 балла из 10 возможных. Брешь отнесли к среднему уровню опасности, поскольку она имеет локальный характер и дает доступ только к учетным записям с низкими привилегиями. При этом Cisco классифицировала ее как «критическую»…

Ввиду этого Cisco, выпустившая новые патчи для устранения ошибки CVE-2018-0141, настаивает на их скорейшей установке владельцами софта PCP. К счастью, баг был обнаружен только в версии 11.6 продукта.

Причиной второй уязвимости (CVE-2018-0147), которой Cisco присвоила уровень «критическая», является ошибка Java-десериализации. Она связана с работой устаревшей системы контроля доступа Cisco Secure Access Control System.

Ее изъяли из продажи еще в августе 2017 года, однако она до сих пор поддерживается…

Остальные 20 обнаруженных уязвимостей получили более низкий рейтинг угрозы. Информацию по ним можно найти на интернет-портале Cisco, посвященном вопросам безопасности…» ***(Julia Glazova. Cisco заявила о двух критических ошибках в своих продуктах // Threatpost (https://threatpost.ru/cisco-patched-2-critical-bugs/25000/). 14.03.2018).***

***

«Компания Microsoft закрыла 15 критических уязвимостей в рамках мартовского вторника патчей. Всего производитель ПО выпустил 75 исправлений, 61 из которых отнесено к важным. Наиболее срочные заплатки получили браузеры Microsoft и связанные с ними технологии, в частности фирменный JavaScript-движок Chakra.

Из 21 браузерного патча 14 являются критическими. При этом одна из заплаток для скриптового движка устраняет сразу 14 багов повреждения памяти.

В бюллетене Microsoft отмечено, что все новые проблемы в Chakra связаны с обработкой объектов в памяти…

В пакет патчей за текущий месяц также включено дополнительное обновление к уязвимостям Meltdown. Теперь меры противодействия эксплойту Meltdown и Spectre реализованы и для 32-разрядных версий Windows 7 и 8.1, а также для Windows Server 2008 и 2012…

Есть и другие исправленные ошибки, достойные упоминания. В их числе — важная уязвимость удаленного выполнения кода (CVE-2018-0886) в протоколе Microsoft Credential Security Support Provider (CredSSP), организующем цепочку аутентификации пользователя при переходе между клиентами...

В пакете Microsoft Office разработчик закрыл 13 багов, связанных с SharePoint, как отмечено в блоге Zero Day Initiative (ZDI). Все недоработки касаются санации ввода и открывают возможность для межсайтового скриптинга (XSS)…» ***(Tom Spring. Microsoft исправила 15 критических багов // Threatpost (https://threatpost.ru/microsoft-patches-15-critical-bugs-in-march-patch-tuesday-update/25013/). 15.03.2018).***

***

«В сети появилась новая версия браузера Chrome. Релиз 65.0.3325.146 закрывает 45 уязвимостей, 9 из которых имеют наивысший рейтинг. В целях безопасности Google раскрывает подробности ошибок только через 14 недель после их исправления. В данный момент детальная информация о багах недоступна, и об их серьезности можно судить лишь по суммам вознаграждений, которые компания выплатила исследователям.

Если использовать в качестве критерия оценки гонорары программы bug bounty, наибольшую угрозу представляют две ошибки в работе с flash-контентом. За обнаружение каждой из них эксперт из Китая получил по $5000…

Еще одна подобная брешь закрыта в движке Blink… Ошибка, обнаруженная в ноябре прошлого года, оценена в $3000.

Свежая версия браузера от Google использует новый V8 Engine — механизм работы с языком JavaScript. Похоже, что еще на этапе тестирования специалисты отловили в нем несколько багов, которые были затем исправлены в финальном релизе. На долю высокопроизводительного движка пришлись три опасные уязвимости, обнаруженные сторонним исследователем и командой Google Project Zero.

Серьезные бреши закрыты в графической библиотеке Skia, механизме обработки 3D-изображений WebGL и утилите PDFium. Разработчики также подлатали компоненту OmniBox, которая отвечает за универсальную адресную строку. Уязвимость, связанная с возможностью подмены url-ссылки, получила средний рейтинг опасности.

Помимо работы с баг-листом, авторы добавили в Chrome новый функционал, напрямую связанный с интернет-безопасностью. В новой версии браузера впервые появилась блокировка страниц, которые используют tab-under…

Google планомерно борется с недобросовестной рекламой. В предыдущей версии браузера отключили редирект по тегу <iframe>, с помощью которого можно было создавать новые секции внутри оригинальной страницы, а также открывать сторонние сайты, не меняя информацию в адресной строке.

Еще одним шагом стала блокировка объявлений, не соответствующих принципам Коалиции за лучшую рекламу. Встроенный механизм удаляет сообщения, которые полностью или частично перекрывают оригинальный контент и автоматически воспроизводят видеоролики с включенным звуком» ***(Julia Glazova. Свежая версия Chrome закрыла 45 уязвимостей // Threatpost (https://threatpost.ru/new-google-chrome-release-patches-45-vulnerabilities/24958/). 12.03.2018).***

***

«Эксперт по веб-безопасности Йосип Франькович (Josip Franjković) помог социальной сети Facebook устранить серьезные бреши в официальном Android-приложении. Уязвимости, которые специалист обнаружил в 2017 году, позволяли злоумышленникам увидеть закрытый список друзей и фрагменты пользовательских платежных данных.

Обе проблемы были связаны с открытым языком GraphQL, созданным Facebook для обработки информации в своих мобильных приложениях…

Все уязвимости были устранены еще в 2017 году. При этом ошибку с раскрытием платежных данных разработчики Facebook исправили буквально за 4 часа — по словам эксперта, с такой быстрой реакцией он не сталкивался ни разу за всю свою карьеру багхантера.

В обоих случаях Франькович взаимодействовал с соцсетью через ее программу отлова ошибок. Размер награды, которую он получил за свой труд, не раскрывается. Однако ранее компания Facebook уточняла, что в общей сложности в 2017 году заплатила багхантерам почти 900 тыс. долларов…» ***(Julia Glazova. Опубликовано описание серьезных уязвимостей Facebook // Threatpost (https://threatpost.ru/two-vulnerabilities-in-facebook/25017/). 15.03.2018).***

***

«Обнаружен ряд серьёзных уязвимостей в популярных смарт-камерах, которые часто используются в качестве видеоняни, а также для наблюдения за обстановкой дома или в офисе. Найденные бреши могли бы позволить злоумышленникам получить удалённый контроль над камерами и делать с ними всё что угодно: от запуска вредоносного кода до выведения их из строя.

Эксперты «Лаборатории Касперского», сообщившие об уязвимостях, передали подробную информацию производителю устройств (Hanwha Techwin): к настоящему моменту часть из них закрыта, оставшиеся будут исправлены в ближайшее время…

Во время своего исследования эксперты «Лаборатории Касперского» обнаружили в облачном сервисе почти 2000 смарт-камер. Однако учитывая, что часть устройств работает через роутеры и файерволы, уязвимых гаджетов может быть в разы больше…

В Hanwha Techwin отметили, что безопасность пользователей является высшим приоритетом для компании. Производитель смарт-камер уже закрыл ряд уязвимостей, в том числе возможность удалённой загрузки и выполнения вредоносного кода. Также компания выпустила обновление прошивки для всех камер и в ближайшее время планирует исправить уязвимости облачного сервиса» ***(В популярных умных камерах обнаружены серьёзные уязвимости // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5480113-V-populyarnyx-umnyx-kamerax-obnaruz.html#ixzz5AC0a8I00). 13.03.2018).***

***

«Новые модели яхт, включающие в себя IoT-устройства с маршрутизаторами и коммутаторами, могут быть взломаны, как и любое другое устройство с подключением к Интернету. Как сообщил исследователь безопасности Стефан Герлинг (Stephan Gerling) на саммите по кибербезопасности в Канкуне (Мексика), у современных яхт есть множество уязвимостей, которые могут потенциально быть проэксплуатированы злоумышленниками, например, бортовой маршрутизатор, имеющий незащищенный протокол FTP…

В рамках презентации Герлинг открыл приложение для управления яхтой (модель яхты и маршрутизатора не раскрываются) на планшете, телефоне и на компьютере, а затем подключился к маршрутизатору и загрузил XML-файл, содержащий конфигурацию маршрутизатора. В частности, исследователю удалось получить учетные данные маршрутизатора, SSID Wi-Fi-сети, а также пароль. По словам специалиста, поскольку файл передается по небезопасному протоколу FTP, он может быть с легкостью перехвачен хакерами, после чего злоумышленники смогут полностью контролировать маршрутизатор и сеть…

После презентации Герлинга на саммите производитель яхт, чье программное обеспечение было использовано, выпустил исправление, устраняющее некоторые из перечисленных проблем безопасности…» ***(Современные яхты уязвимы к кибератакам // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122023). 19.03.2018).***

***

«В рамках конференции Kaspersky Security Analyst Summit в Канкуне (Мексика) исследователи безопасности из компании IOActive продемонстрировали атаку с использованием вымогательского ПО на роботов…

Эксперты Сезар Серрудо (Cesar Cerrudo) и Лукас Апа (Lucas Apa) продемонстрировали атаки на доступных в продаже роботах Pepper и NAO от SoftBank Robotics. В настоящее время по всему миру продано более 30 тыс. данных моделей.

Атака с использованием вымогательского ПО на робота отличается от атаки на компьютер главным образом тем, что робот обычно не хранит данные, а только обрабатывает их. Несмотря на это, подобная атака может привести к потере доступа к данным, прекращению производства или сбоям в работе до тех пор, пока робот не будет исправлен.

Исследователи безопасности создали собственное вымогательское ПО для атаки на модель NAO, однако оно работает и на модели Pepper. Как показали эксперты, выполнив собственный код в любом из классов, в том числе в файлах поведения, можно заставить робота осуществлять вредоносные действия…» ***(Исследователи заразили роботов вымогательским ПО // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=121893). 13.03.2018).***

***

«Эксперт в сфере информационной безопасности Дор Азури из компании SafeBreach провел анализ популярных текстовых редакторов для систем Linux и Unix, в ходе которого выявил в большей части из них уязвимости, которые дают хакерам возможность повышать привилегии и выполнять вредоносный код на компьютерах жертв. Так, проблемы присутствуют в текстовых редакторах Emacs, Gedit, Sublime и Vim.

В отчете указано, что данная методика является успешной вне зависимости от того, открыт ли какой-нибудь файл в редакторе, потому никакие ограничения могут не защитить программу…

Азури советует пользователям Unix применять систему обнаружения вторжений, имеющую открытый исходный код OSSEC, для того, чтобы вести мониторинг активности системы, целостности файлов, журналов и процессов.

Пользователям также не стоит загружать сторонние плагины, если редактор работает с повышенными привилегиями.

Кроме того, Азури рекомендует разработчикам текстовых редакторов заменить папки и модели разрешений файлов для разделения между режимами, а также вручную добавить интерфейс для одобрения загрузки плагинов с повышенными привилегиями» ***(Хакеры могут повышать привилегии на системе с помощью плагинов в текстовых редакторах // SecureNews (https://securenews.ru/safebreach/). 16.03.2018).***

***

«Ученые Университета имени Бен-Гуриона нашли новый способ извлекать данные с физически изолированных компьютеров, используя колонки и наушники. Пока что метод, получивший название MOSQUITO, не применялся в реальных атаках.

Он предполагает применение техники, которая известна как jack retasking (переназначение аудиоразъемов), что дает возможность заставлять динамик работать по принципу микрофона…

Как утверждают эксперты, вредоносная программа, установленная на физически изолированном компьютере, может преобразовывать локальные файлы в аудиосигналы и передавать их на другое устройство посредством подключенных колонок или наушников. Затем второй компьютер, который также заражен вредоносной программой, используя технику jack retasking, «превращает» колонки или наушники в микрофон, принимает сигнал и восстанавливает отправленный ранее файл.

Эксперты создали протокол, который конвертирует двоичные данные в аудиосигналы, и испытали эту методику на расстоянии от 1 до 9 метров. Скорость передачи данных с одного компьютера на другой варьировалась от 1200 бит в секунду до 1800 бит в секунду в ходе эксперимента, когда колонки были размещены друг напротив друга и издавали звук в диапазоне, воспринимаемом человеком (ниже 18 килогерц).

Снижение скорости передачи данных происходило, если колонки были повернуты в разные стороны, возрастало расстояние между ними, менялась частота аудиосигнала или применялись наушники…» ***(Найден новый способ извлечения данных с физически изолированных компьютеров // SecureNews (https://securenews.ru/mosquito_2/). 13.03.2018).***

***

«Свыше 50% почтовых серверов находятся под угрозой ввиду критической уязвимости в агенте передачи сообщений Exim, который применяется в операционных системах семейства Unix.

Эта программа функционирует на почтовых серверах и ее задачей является передача электронных сообщений…

Уязвимость обнаружил тайваньский исследователь информационной безопасности, известный как Meh. Она дает хакеру возможность обманывать сервер Exim и выполнять вредоносные команды до того, как злоумышленнику понадобится пройти авторизацию на сервере. Уязвимость носит характер однобайтового переполнения буфера в функции декодирования base64. Данная проблема присутствует во всех версиях Exim.

Эксперты передал информацию о проблеме разработчикам Exim в начале февраля… Разработчики уже выпустили версию Exim 4.90.1, в которой проблема устранена…» ***(Уязвимость в Exim несет угрозу для сотен тысяч почтовых серверов // SecureNews (https://securenews.ru/exim/). 07.03.2018).***

***

«Издание 9to5mac сообщает, что компания Grayshift создала девайс GrayKey, который сумел разблокировать iPhone, не зная пароля…

GrayKey внешне практически не отличается от Apple TV — это такая же серая коробка, только с парой коннекторов для подключения iPhone. На взлом одной трубки у него уходит от 2 часов до 3 суток в зависимости от сложности пароля… Девайс создали несколько бывших инженеров Apple и специалистов по кибербезопасности, которые работали в спецслужбах.

...GrayKey — это никак не устройство для массового рынка и просто так купить его не получится. Вместо этого Grayshift предлагает услуги по взлому iPhone — за $15 000 взломают iPhone, подключенный к конкретной сети, за $30 000 — чуть ли не какой угодно. Более подробно про программный процесс взлома западные источники, к сожалению, ничего не рассказывают…» ***(Евгений Щербань. Бывшие инженеры Apple создали гаджеты для взлома iPhone — GrayKey // gagadget.com (http://gagadget.com/announce/34528-byivshie-inzheneryi-apple-sozdali-gadzhetyi-dlya-vzloma-iphonegraykey/). 17.03.2018).***

***

«…Компания Microsoft выпустила внеплановое обновление безопасности для 64-разрядных версий Windows 7 и Windows Server 2008, которое призвано исправить проблемы, вызванные январским патчем для уязвимости Meltdown (CVE-2017-5754).

Как ранее сообщил шведский специалист Ульф Фриск (Ulf Frisk), патч, выпущенный в рамках январского «вторника исправлений», привел к более критичной уязвимости, позволяя любому пользовательскому приложению читать содержимое из ядра операционной системы, а также записывать данные в память ядра. Ульф обнаружил проблему, работая над устройством PCILeech, созданном для проведения атак с прямым доступом к памяти (DMA) и дампу защищенной памяти операционной системы.

По его словам, исправление Meltdown случайно перевернуло бит, контролирующий права памяти для памяти ядра. Данной уязвимости был присвоен идентификатор CVE-2018-1038. Проблема затронула только 64-битные версии Windows 7 и Windows Server 2008 R2. Microsoft исправила уязвимость, переопределив бит разрешения PML4 в исходное значение в патче 2018-3.

По словам Фриска, патч, судя по всему, устраняет уязвимость, так как после его установки исследователь не смог взаимодействовать с памятью ядра. Однако 29 марта Microsoft выпустила еще одно обновление, KB4100480 , чтобы полностью устранить проблему…» ***(Microsoft выпустила внеплановый патч для Windows 7 и Windows Server 2008 // SecurityLabRu (https://www.securitylab.ru/news/492362.php). 30.03.2018).***

***

«… Консорциум промышленного интернета (Industrial Internet Consortium, IIC) разработал руководство, призванное упростить безопасность «Интернета вещей» (IoT). Документ получил название «Endpoint Security Best Practices» («Лучшие практики по обеспечению безопасности конечных точек»).

Конечные точки IoT включают в себя такие устройства, как датчики, приводы, насосы, расходомеры, контроллеры и приводы в промышленных системах; встроенные медицинские приборы; электронные блоки управления; системы управления транспортными средствами; инфраструктура связи и шлюзы. Вышеперечисленные устройства, как правило, разработаны без учета требований кибербезопасности. Они содержат вшитые неизменяемые пароли, а их настройки по умолчанию предполагают подключение к интернету.

С целью помочь администраторам улучшить безопасность этой части сети IIC разработала 13-страничный краткий документ для производителей оборудования, операторов критической инфраструктуры, системных интеграторов и пр. Документ представляет собой справочную информацию по внедрению контрмер и средств контроля для обеспечения безопасности и надежности конечных IoT- устройств…» ***(IIC представил руководство по обеспечению безопасности конечных точек IoT // SecurityLabRu (https://www.securitylab.ru/news/492022.php). 13.03.2018).***

***

«Лаборатория Касперского» предлагает ИБ-специалистам до 100 тыс. долларов за обнаружение критической уязвимости в своих продуктах…

Взломщикам предлагается работать с новейшими бета-версиями основных продуктов «Лаборатории Касперского» — Kaspersky Internet Security 2019 и Kaspersky Endpoint Security 11. Наибольший бонус (20–100 тыс. долларов) получат хакеры, которые смогут удаленно выполнить код на пользовательской машине через канал обновления баз…

Прочие способы выполнения кода в процессе с высокими привилегиями принесут взломщику 5–20 тыс. долларов. Если специалист получит доступ к пользовательским конфиденциальным данным или найдет другие ошибки, он сможет рассчитывать на выплату до десяти тысяч долларов — в зависимости от типа и сложности уязвимости.

В своем сообщении «Лаборатория Касперского» уточнила, что за полтора года с момента запуска программы «белые» хакеры нашли в ее продуктах более 70 ошибок, которые были затем исправлены…

В январе журналисты «Ведомостей» узнали, что российское правительство планирует запустить собственную программу по поиску уязвимостей в отечественных и зарубежных ИТ-системах. На эти цели предполагается выделить

800 млн рублей. По информации журналистов, некоторые продукты будут предложены хакерам без предварительного уведомления их разработчиков.

Багхантинговая инициатива «Лаборатории Касперского» входит в программу информационной открытости, которая была запущена в октябре 2017 года. В ее рамках независимые эксперты получат доступ к исходному коду продуктов компании, включая код обновлений ПО и антивирусные базы.

Программа также включает планы открыть к 2020 году три Центра прозрачности (Transparency Centers) в Азии, Европе и США, где клиенты и партнеры компании и представители госорганов смогут получить информацию о программном коде, обновлениях продуктов, антивирусных базах и решить другие вопросы кибербезопасности» ***(Julia Glazova. Белые хакеры смогут заработать 100 тыс. долларов // Threatpost (https://threatpost.ru/kaspersky-lab-offers-100-thousand-dollars-bug-bounty/24963/). 12.03.2018).***

***

«Чтобы сократить время обнаружения злоумышленников, специалисты по кибербезопасности все больше применяют (и закупают) средства, использующие искусственный интеллект и машинное самообучение.

Вредоносное ПО не перестает совершенствоваться: сегодня злоумышленники используют облачные сервисы и избегают обнаружения с помощью шифрования, которое помогает скрыть активность потока команд и управления…

Применение машинного самообучения (МС) помогает повысить эффективность защиты сети и с течением времени позволит автоматически выявлять нестандартные паттерны в шифрованном веб-трафике, в облачных и IoT-средах. Некоторые из 3600 директоров по информационной безопасности, опрошенных в ходе подготовки отчета Cisco 2018 Security Capabilities Benchmark Study, заявили, что доверяют таким инструментам, как МС и ИИ, и хотели бы их использовать, но они разочарованы большим количеством ложных срабатываний. Технологии МС и ИИ, которые сейчас находятся в самом начале своего развития, с течением времени усовершенствуются и научатся определять «нормальную» активность сетей, мониторинг которых они осуществляют. Тем не менее 39% организаций делают ставку на автоматизацию, 34% — на машинное самообучение, 32% — на искусственный интеллект…

Некоторые результаты отчета Cisco 2018 Annual Cybersecurity Report

…По данным респондентов, более половины всех атак нанесли финансовый ущерб в размере свыше 500 млн долларов, включая в том числе потерю доходов, отток заказчиков, упущенную выгоду и прямые издержки.

Такие атаки способны масштабно поражать компьютеры, при этом их действие может продолжаться месяцы и даже годы…

Для своей защиты организации используют комплексные сочетания продуктов от различных производителей. Такое усложнение при расширяющемся разнообразии уязвимостей отрицательно сказывается на способность организаций к отражению атаки и ведет в том числе к увеличению рисков финансовых потерь.

В 2017 г. 25% специалистов по информационной безопасности сообщили, что используют продукты от 11—20 вендоров, в 2016 г. так ответили 18%.

Специалисты по информационной безопасности сообщили, что 32% уязвимостей затронули более половины систем, в 2016 г. так ответили 15%...

Растет использование облачных технологий; атакующие пользуются отсутствием продвинутых средств обеспечения безопасности

В этом году 27% специалистов по информационной безопасности сообщили об использовании внешних частных облаков (показатель 2016 г. — 20%).

Из них 57% размещают сеть в облаке ради лучшей защиты данных, 48% — ради масштабируемости, 46% — ради удобства эксплуатации.

Хотя облако и обеспечивает повышенную безопасность данных, атакующие пользуются тем, что организации не очень хорошо справляются с защитой развивающихся и расширяющихся облачных конфигураций…

Продемонстрированное Cisco медианное время обнаружения (time to detection, TTD) за период с ноября 2016 по октябрь 2017 г. составило около 4,6 часов. В ноябре 2015 г. этот показатель составил 39 часов…

Ключевым фактором для Cisco в процессе сокращения времени обнаружения и поддержания его на низком уровне стали облачные технологии обеспечения информационной безопасности. Чем меньше время обнаружения, тем быстрее отражается атака…» ***(Кибербезопасность требует новых подходов // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5480103-Kiberbezopasnost-trebuet-novyx-podx.html#ixzz5ABy7jUL3). 13.03.2018).***

***

«Команда исследователей кибербезопасности создала автоматизированный анализатор вредоносных программ для macOS, который упрощает процесс обнаружения и изучения растущего количества вредоносного ПО, ориентированного на компьютеры от Apple…

По словам аналитика Фам Дуй Фука (Pham Duy Phuc) из компании Sfylabs BV, ранее исследовательские инструменты для macOS, как правило, основывались на ручном анализе вредоносного ПО. Данное положение дел подтолкнуло его начать разработку инструмента, получившего название Mac-A-Mal…

Mac-A-Mal использует комбинацию статического и динамического анализа кода для обнаружения вредоносного ПО, а также для обхода методов антианализа, которые некоторые авторы вредоносного ПО используют для предотвращения обнаружения. Инструмент собирает двоичные шаблоны поведения вредоносных программ, такие как сетевой трафик, методы маскировки и операции с файлами…

Исследователи использовали инструмент для анализа примерно 2 тыс. образцов вредоносов для Mac на VirusTotal, что привело к обнаружению ранее неизвестной рекламной кампании, в которой используются законные сертификаты Apple, кейлогеры и трояны.

…команда также обнаружила сотни других образцов вредоносных программ для Mac, которые было бы трудно идентифицировать с помощью ручных инструментов…» ***(Разработан инструмент для поиска и анализа вредоносов для Mac // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=121956). 15.03.2018).***

***

«…Latvijas Mobilais Telefons (LMT), крупнейший в стране оператор мобильной связи Латвии, приглашает исследователей протестировать выбранное им кибероружие в своей сети – а точнее, в специально построенном для этих целей сегменте Mobile Cyber Range.

…полигон LMT Mobile Cyber Range, как и любой традиционный тир, является местом проверки оружия – в данном случае вредоносных программ, проникающих в беспроводные сети телекоммуникационных операторов и подключаемых к ним мобильные устройства, без причинения какого-либо вреда кому бы то ни было в реальном мире…

LTM может смоделировать все, что угодно, начиная от элементов инфраструктуры базовой сети и заканчивая беспроводными передатчиками и SIM-картами мобильных устройств. Первоначально LMT ориентировалась на системы Nokia, своего собственного поставщика оборудования, но в дальнейшем компания планирует поддерживать и оборудование других поставщиков.

Моделирование всей мобильной сети оператора – несколько более сложная задача по сравнению с запуском виртуальной машины, игравшей роль ПК или сервера, поскольку для этого необходимо специальное оборудование, которое будет имитировать работу элементов беспроводной сети…» ***(Питер Сойер. Мобильный оператор приглашает кибервзломщиков // ООО «Издательство «Открытые системы» (https://www.computerworld.ru/articles/Mobilnyy-operator-priglashaet-kibervzlomschikov). 15.03.2018).***

***

«В среду корпорация Google анонсировала набор новых функций безопасности для Google Cloud Platform и G Suite…

Для Google Cloud Platform были реализованы службы управления виртуальным приватным облаком VPC Service Controls. В настоящее время в альфа-версии представлен файрвол для основанных на API служб, а также функции защиты данных от утечки в случае проникновения злоумышленника в систему…

Компания также запускает инструмент Cloud Security Command Center, который дает компаниям более глубокое представление о защищенности их данных в облачных сервисах Google. Его основная функция заключается в том, чтобы помочь компаниям собрать данные, оценить угрозы и принять меры до того, как данные будут скомпрометированы или потеряны…

Компания также уделила больше внимания противостоянию атакам DDoS и защите приложений, для чего был запущен сервис Cloud Armor. Cloud Armor предлагает инструменты белых и черных списков, а также интегрируется с сервисом Cloud HTTP(S) Load Balancing.

Что касается G Suite, то здесь корпорация реализовала новые функции антифишинга. Google добавила машинное обучение, которое будет автоматически помечать подозрительные электронные письма с зашифрованными вложениями или встроенными скриптами…» ***(Олег Иванов. Google совершенствует инструменты безопасности в Google Cloud, G Suite // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-03-22-1447/25787). 22.03.2018).***

***

«…председатель совета директоров и главный технологический директор компании Ларри Эллисон объявил о выпуске первого сервиса на основе новой автономной базы данных Oracle Autonomous Database.

Первый в мире облачный сервис, по заявлению производителя, Oracle Autonomous Data Warehouse Cloud, соответствующий принципам самоуправления, самозащиты и самовосстановления, использует машинное обучение для достижения лучших в отрасли показателей производительности, безопасности и доступности — без вмешательства человека…

Автономная база данных представляет собой совершенно новый класс предложений, который не требует во время работы администрирования со стороны клиента. Такое облачное хранилище данных обладает следующими характеристиками:

Простота в работе…

Высокопроизводительность…

Эластичность…

В течение текущего календарного года Oracle планирует предоставить автономные сервисы Oracle Autonomous Analytics, Oracle Autonomous Mobility, Oracle Autonomous Application Development и Oracle Autonomous Integration» ***(Oracle представила первую в мире автономную базу данных // «Компьютерное Обозрение»(http://ko.com.ua/oracle_predstavila_pervuyu_v_mire_avtonomnuyu_bazu_dannyh_124051). 28.03.2018).***

***

Нові надходження до Національної бібліотеки України імені В.І. Вернадського

Верховенство права очима правників-початківців : матеріали Всеукр. наук. конф. студентів та аспірантів, 3 груд. 2016 р., м. Одеса. - Одеса : Юридична література, 2016. - Т. 2. - 407 с.

Зі змісту:

- Борбелюк В.П. Реалізація стратегії кібербезпеки України як складова оптимізації протидії злочинності у мережі Іетернет.

Шифр зберігання НБУВ: В356889/2.

***

Діяльність підрозділів карного розшуку Національної поліції України щодо протидії злочинам проти власності, особливо корисливо-насильницьким у сучасних умовах : зб. матеріалів постійно діючого семінару "Методологічні проблеми теорії та практики оперативно-розшукової діяльності в сучасних умовах" (1-3 черв. 2017 р.). - Луганськ : РВВ ЛДУВС ім Е. О. Дідоренка, 2017. - 195 с.

Зі змісту:

- Березовська А.Р., Бараненко Р.В. До питання визначення криміналістичної характеристики відмивання доходів від кіберзлочинів.

Шифр зберігання НБУВ: ВА817006.

***

Лисенко С.М. Метод виявлення кібер-загроз на основі еволюційних алгоритмів / С.М. Лисенко, Д.І. Стопчак, В.В. Самотес // Вісник Хмельницького національного університету. Технічні науки. - 2017. - № 6 (255). - С. 81-88.

Представлено метод, який дозволяє забезпечити реагування на нові загрози, забезпечуючи захист комп'ютерних систем від як відомих, так і невідомих кібер-загроз.

Шифр зберігання НБУВ: Ж69410.

***

Міжнародна інформаційна безпека: теорія і практика : підруч. для студентів ВНЗ, які навчаються за напрямом підгот. "Міжнародні відносини" та "Міжнародна інформація". - Київ : Центр вільної преси, 2016. - 417 с.

Присвячено теоретичним та прикладним дослідженням міжнародної інформаційної безпеки та кібербезпеки. Подано тлумачення осносних понять міжнародної інформаційної безпеки. Охарактеризовано сучасні теорії інформаційної безпеки та інформаційного протиборства. Розглянуто класифікацію інформаційних та кіберзагроз для системи міжнародної безпеки.

Шифр зберігання НБУВ: ВА816855.

***

Правове регулювання ІТ-відносин : матеріали Всеукр. круглого столу, 18 трав. 2017 р. - Одеса : Фенікс, 2017. - 85 с.

Зі змісту:

- Григор'янц Г.І. ІТ-піратство та інформаційна безпека.

Шифр зберігання НБУВ: ВА816444.

***

Проблеми інформатики та комп'ютерної техніки (ПІКТ - 2017) = Проблемы информатики и компьютерной техники (ПИКТ - 2017) = Informatics and computer technics problems (PICT - 2017) : пр. VI-ї Міжнар. наук.-практ. конф., 5-8 жовт. 2017 р. - Чернівці, 2017. – 170 с.

Зі змісту:

- Киричек Г.Г., Сергєєв О.Д. Система захисту передачі інформації;
- Кузнецов А.А., Ахметов Б.С., Ташимова А.К. Современные проблемы информационной безопасности.

Шифр зберігання НБУВ: СО35482.

***

Тези доповідей VI Міжнародної науково-практичної конференції "Інформаційні технології в освіті, науці і виробництві (ІТОНВ-2017)", м. Луцьк, 25-27 травня 2017 р. - Луцьк : Луц. НТУ, 2017. - 235 с.

Зі змісту:

- Мельник К.В., Лотоцький І.М., Мельник В.М., Багнюк Н.В. Нейромережевий детектор відстеження вірусних атак;
- Кабак В.В., Костючко С.М. Кібербезпека як фактор забезпечення національної системи захисту кіберпростору;
- Панасюк Н.Л., Парфенюк Ю.О. Захист даних в WI-FI мережах;
- Поліщук М.М., Гринюк С.В., Хома М.Д. Комп'ютерна підсистема сигналізації несанкціонованого доступу до автомобіля.

Шифр зберігання НБУВ: ВА816687.

***

Ярощук Д.О. Удосконалення методу обрахунку впливу загроз інформаційної безпеки на ефективність функціонування закритої телекомунікаційної мережі / Д.О.Ярощук // Вісник Хмельницького національного університету. Технічні науки. - 2017. - № 6 (255). - С. 66-69.

Розглянуто завдання забезпечення ефективного функціонування телекомунікаційних мереж. Представлено методи оцінки захищеності об'єктів мережі від загроз інформаційної безпеки.

Шифр зберігання НБУВ: Ж69410.

***

Виготовлено в друкарні
ТОВ «Видавничий дім «АртЕк»
04050, м. Київ, вул. Мельникова, буд. 63
Тел.. 067 440 11 37
artek.press@ukr.net
www.artek.press

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції –
серія № ДК №4779 від 15.10.14р.